Experience Summary
James E. Lukaszewski ABC, APR, Fellow PRSA

CYBER-ATTACKS, BREACHES, SOCIAL MEDIA PROBLEMS

The Lukaszewski Group plays one some or all of seven key roles during these crisis scenarios:

1. Detection (monitoring and analysis), deterrence, preemption, and communication response strategies
2. Victim management guidance, contention reduction
3. Readiness, including exercises and drills
4. Preparing leadership to understand, anticipate, and to promptly and constructively respond
5. Destiny management . . . if the client fails to do it, someone else will
6. Trap avoidance: those behaviors and decisions that tarnish reputation, empower victims and create career defining moments for leaders. These operational and reputational traps include:
   - Trap 1. Silence, nondisclosure, disclosure, delay: the most toxic strategies of all
   - Trap 2. Acting like a victim . . . it's your customers, employees, innocent bystanders who are the victims
   - Trap 3. Searching for perfect responses, takes too long, reputation in tatters by the time you find it, if it ever is found.
   - Trap 4. Ignoring the high level of media and victim knowledge of the event patterns. Response expectations, especially of important companies, are getting higher.
   - Trap 5. Failure to promptly, thoroughly and sincerely apologize for inconvenience, fear, uncertainly and worries
   - Trap 6. Do less than expected, delay key, or any sensible action decisions.
   - Trap 7. Demean, diminish, discredit or minimize the damage, the critics, bloviators, or the self-appointed
   - Trap 8. Fail to act promptly and decisively fearing litigation consequences.
7. Web based strategies to respond, inform, correct and clarify, expose and comment on the unartful, the mistaken, the half-truth and the fantasies.

The Lukaszewski Group provides constructive, preemptive, and sensible victim managing response advice:

1. Bad news ripens badly; get ahead of it because we know the pattern of events about to occur
2. Speed of response and action beats smart but delaying thinking every time
3. Stop the production of victims
4. Manage the victim dimension
5. Notify, disclose, explain, and be candid
6. Work constructively and preemptively against the pattern of events
7. Voice extreme empathy, even apology for those affected.
8. Communicate constructively, openly, incrementally, daily or more frequently.
9. Correct, clarify, and comment promptly . . . it is your destiny.
10. Criticisms of your performance are predictable, inevitable and correctable.

Types of breaches and cyber-attack situations The Lukaszewski Group has been involved in over the years:*

- Consumer Breaches-Travel and Tourism
- Consumer Breaches-Retail
- Social media attacks on individuals, consumer products and brands, Public and private institutions, industries
- Organized opposition: increasing use of cyber tools to recruit, align and coordinate forces that enjoy anonymously harassing, irritating, agitating, and humiliating.

* All Lukaszewski Group clients are confidential.

The 2014 Target Stores Breach
An Unusual Case Study

Although I know a number of people who work in communications and management at Target, I have never had an official business relationship with them. They are headquartered in Minneapolis and St. Paul where my business headquarters is also located.

As the Target breach story began to unfold, they were, of course, under attack by everybody including pundits, bloviators, anybody wanting to get their name in the paper or on the web. I wrote a brief blog treating Target's breach response in a highly positive way. Since my voice was the only one being complementary, I naturally became the subject of news interviews. The purpose of these interviews was primarily to have me eat my words.

One local television station asked me in two different interviews to describe just how badly the CEO was performing. My response was to explain exactly what was happening in the C-suite at Target (although I never was there, nor was I contacted by the company). I have been through this scenario many times in the past. I talked about the stresses and strains this type of story is on organizations like Target, their leadership, management, employees, shareholders and other stakeholders. I also described precisely what was going on in the C-suite, besides no sleep, enormous tension and the search to do something good and reassuring for customers.

Despite the tremendous media pressure and terrifying daily expansion of the numbers of those affected and victimized by the breach, the company seemed to be setting up and doing the kinds of things that it could do, within the constraints of operating in a crime scene, and becoming the subject of global scrutiny.

This is indeed the pattern of breaches. There have been so many, and they are now so frequent, it is the foolish company that attempts to defer, deny, delay action, or attempt to discredit victims, demean those on the attack, deplore the overwhelming coverage, and live in a state of denial.

It's true, Target at first listened to the police and their attorneys, deciding to delay announcing their situation until it was outed by a blogger. After that, Target could not seem to catch up. However, as one familiar with these kinds of events, they still performed pretty admirably under the circumstances.

Predictably, and in Target's case extraordinarily, internal legal counsel were the first casualties. Uncharacteristically, there was a change in communication leadership, IT leadership, then the chief executive, and a significant number of board members.

This approach is one I described as, "Ready and Fire Aimlessly."

The great irony of this story is that experts tend to agree that the Target situation was unpreventable until it had occurred. Most reputable consultants admitted, after castigating Target for all kinds of problems, issues and mistakes, that the nature of hacking is like trying to defeat an army of beavers, squirrels, chipmunks and groundhogs, animals who chew on some part of your property literally 24 hours a day, seven days a week.

The reality is and will continue to be that if you come under attack, regardless of the defenses you direct, the cyber beavers, raccoons, chipmunks, groundhogs and squirrels will find and exploit your weaknesses.

The lesson is that in addition to having the smartest, savviest and aggressive cyber defenders, it is even more essential to recognize the patterns of public, government, industry, and social response when breaches occur. And, to be as aggressive as possible in managing and maintaining a relationship of trust with all of your key stakeholders, keeping your balance, and to recognize that the communication and behavior formula described above is the formula for victory, and reputational damage mitigation.