CYBERCRIME IS REWRITING THE RULES OF CRISIS MANAGEMENT

NEW ORDER OF MAGNITUDE

Cybercrime represents a whole new order of magnitude of crisis for every organization and industry around the world. No company large or small, no bank or financial institution, hospital, insurer, university, nonprofit or government is immune.

Now that cybercrime is such big business, organized crime, global governments, and loose confederations of hacktivists attack organizations relentlessly to take over customers' identities, finances, smart homes, cars, insurance benefits, tax returns, electrical and water supply, lives. Commenting on a recent bank cyberattack, Preet Bharara, the U.S. Attorney for the Southern District of New York, called the breaches "breathtaking in scope and in size," signaling a "brave new world of hacking for profit," or "securities fraud on cyber steroids."

And it is ubiquitous. Even the private email of CIA Director John Brennan has been hacked – by a particularly persuasive hacker talking customer service representatives from Verizon into freely giving out information tied to his account.

Stolen data is being sold not only on the dark web, but on YouTube. And everyone knows this is only the beginning. Identity will be compromised in the future in ways that neither the black nor white hats can even imagine today, using stolen retinal scans, fingerprints, fMRIs and, who knows, possibly even brain waves. (See sidebars on "How Hackers Use Stolen Data" and "How Hackers Will Use Data in the Future (and the Future is Here).")

The repercussions can be staggering:

- The attacks come from the inside and the outside – from friend and foe. They are relentless, profuse, inventive, and sometimes successful.
- Hackers are estimated to have exposed over 100 million people with bank accounts to various schemes generating hundreds of millions of dollars in illicit proceeds, laundered through more than 75 shell companies around the world.
- In reality, there is no way for us to know the total number of breaches that have taken place or the number of consumer records that have been

exposed, since only a portion of breaches are identified. Even among those identified, only one quarter to one third can estimate how many records have been exposed.

- In 2015 alone, the Identity Theft Resource Center reports that 781 major data breaches occurred. Of them, for over 430 breaches, it was not possible to estimate how many records were hacked. Of the 350 breaches where it was possible, 169 million consumer records were exposed. Estimates go as high as 400+ million user records hacked in the last year alone.
- Given that it takes an average of **270 days** before a hack is even discovered, the real number of individuals and entities whose information has been compromised in 2015 is almost certainly far greater.
- Each successful corporate hack costs an organization an average of $3.8 million to address, but the actual cost to a company in lost revenues, lost shareholder value, and lost brand value is much, much more.

TRADITIONAL CRISIS MANAGEMENT IS OBSOLETE

At the same time, most of the ways organizations have successfully handled crises up until now simply do not work anymore.

Cybercrime is literally rewriting the crisis management rule book.

Traditional crisis management techniques may be time-honored, but often they are static, formulaic, siloed, derivative, and constrained – simply not adequate for the dynamic, nuanced, multi-faceted, and ubiquitous nature of cybercrimes today.

Effective cyber crisis management now must straddle the lines between enterprise risk management, information technology, business continuity, emergency response, law enforcement, legal liability, reputation management, and corporate governance.

From the board to executive leadership to those on the front lines, cybersecurity crisis management must include a combination of traditional crisis management techniques and emergency and terrorist response, which necessitates organizations develop internal and external cooperation and communication of an unprecedented nature.

NEW CRISIS MANAGEMENT RULES FOR THE CYBER AGE

So, based upon Temin and Company's significant experience working with almost every kind of organization on cyber crisis – from banks, services firms, and consumer product goods and industrial companies to hospitals, universities and nonprofits – as well as the many keynote speeches and presentations we have delivered to Chief Information Security Officers (CISOs) and other corporate directors and executives, here are 7 new rules of cybersecurity crisis management – geared to an ever-changing reality.

1. **Decisiveness not denial is called for when a breach is discovered.** As corporate boards begin to take far more interest in cybersecurity, and the mishandling of breaches can seriously harm shareholder value as well as the job security of the CEO, the stakes get higher. This can sometimes lead to a paralysis of leadership.

   Whereas with the Tylenol crisis years ago, executives could take three days to decide what to do, executives today do not have that latitude.

   You may first hear about a hack from social media, law enforcement, customers, employees, or

How Hackers Use Stolen Data

1. Sell it as-found on the black market/deep web.
2. Facilitate other attacks, including:
   a. DDoS (Denial of Service)
   b. Phishing
   c. Stealing more data
3. Create fake identities with it to:
   a. Commit insurance fraud
   b. Commit credit card fraud
   c. Sell on the black market/deep web
   d. Empty your bank account
   e. Create fake profiles in your name
   f. File fake tax returns/tax fraud
   g. Social security fraud
4. Use information from email accounts to:
   a. Sell as a list for shady advertisers/scammers
   b. Try to steal your password with phishing scams
   c. Send phishing scams to your email from your contacts and steal your information
   d. Send phishing scams from your email to others to steal their information
   e. Send you viruses
5. Advertise it on YouTube and promote their skills.
6. Infiltrate your social media accounts or website and vandalize them/post on your behalf/place unauthorized advertisements.

traditional print or broadcast media. In these situations, it is critical to not back away, deny, minimize, or go into endless internal meetings. Even if you know very little, it is important to say what you think you know so far – with the caveat that it is still early, promise to find out more as fast as possible, and report what you know as you know it.

Drafting such a "holding statement" can and should be done well before a cybercrisis hits, and should become part of your crisis plan and table top exercises.

This all takes decisive leadership, and usually involves the board, CEO, executive team, and functional experts all working smoothly in real time. There is no room for turf wars – all must have been planned out and practiced beforehand. But the CEO and board, guided by an experienced risk/crisis expert must be prepared to act promptly.

Wisdom comes in neither overreacting nor underreacting to the situation, but in reading it right, and reacting with concern and care for your customers and employees as well as your shareholders.

2. **That said, don't give away your power.** Reporting breaches to law enforcement may seem reflexive, but not every organization chooses to do

How Hackers Use Stolen Data – cont'd

7. Post it online or "dump" the data to publicly shame victims.
    a. Post it on YouTube
    b. Post it in a PasteBin "Dump"
    c. Post it on Twitter
8. Send it to interested journalists.
9. Use it to set up "zombie" or "dummy" accounts or full networks of "zombies" (accounts that seem real but are computer-operated).
    a. For committing fraud
    b. For manipulating online polls and contests
    c. For manipulating markets
    d. To conduct nefarious operations – additional hacking and cyberattacks or character assassinations against people, organizations, or states
10. Blackmail victims
    a. Hold information hostage to manipulate the victims or collect ransom
    b. Sell it to criminals who blackmail the victims
11. Commandeer your devices on the Cloud
    a. Penetrate home security systems
    b. Penetrate public walls such as electrical grids, dams, nuclear facilities, the FAA air traffic control systems, etc.
    c. Infiltrate global stock exchanges, payment systems, settlement exchanges, reporting systems, etc.

so (except for regulated industries, where you must).

Sometimes law enforcement will seek to control the situation in a way that may not be in your best interests. At that time, it is important to know that you are in a negotiation with them (assuming you are not legally culpable), and that you can still insist upon exercising some control. The same is true for your technical advisors – you need them, of course, but do not always have to take their advice.

The best leaders follow their "informed guts" during crisis, even if that is at odds with your advisors or law enforcement. It just cannot be at odds with those adversely affected by the breach, or with your board.

3. **The public may actually not care as much as you think – they are getting used to the breaches, and to the idea that their data is vulnerable. These are becoming facts of life.** The "first movers" in any new kind of cyber crisis will always come under great scrutiny and judgment. But follow-on victims are faring much better. If you show great care, customer solicitousness, and even over-kill in your reaction, you may come out relatively unscathed. Witness how Elon Musk announced the total recall of his electric cars when one part could potentially malfunction: his customers were mollified and the crisis ended swiftly.

4. **How you make an announcement of a breach is just as important as when you make it.** As we have said, the discovery of most breaches is not immediate: on average it takes 270 days before a breach is discovered. By then, the damage has already been done, and the hackers may have even moved on.

   The holy grail of crisis management is to announce a crisis immediately and completely – letting all "shoes drop" at the same time, and then concentrating on the solutions both publicly and privately.

   But when the timing is so disjointed, it can be almost impossible to announce breaches in a "timely manner." Also, your tech teams, as well as law enforcement, may request that you hold off from announcing the breach so that they can attempt to track and catch the criminals. They may or may not be able to do this, but usually they will ask for you to wait for longer than you would like.

   In Europe, legislation is being considered to mandate, for both European companies and any companies that collects data about

Europe's 500 million residents, that they report a breach to a national privacy "watchdog" within 72 hours of finding out about a hack, and then to announce it to consumers quickly thereafter. The US may follow suit with similar legislation.

Therefore, if you can't control the timing, it becomes even more important to concentrate on controlling the message.

Whether or not one chooses to issue a public statement depends upon the magnitude of the breach, and whether it has already leaked out and gained media attention. There is a growing portfolio of tools you can use to post announcements or press releases on your website, or on newly linked "micro sites."

However, it is always prudent to write a personalized and compelling letter from a senior executive of the organization to each customer or employee whose data has been compromised. The letter should provide a 24/7 hotline to answer questions, credit monitoring for some period of time, and offer to help those affected address the repercussions of any identity theft that may result.

As we said before, overkill works. Even if your audiences do not take

How Hackers Will Use Data in the Future (and the Future is Here)

1. Hacking the Internet of Things
    a. Sending a driverless car off course, using it to kill or injure the passenger, or kidnap them and hold them hostage.
    b. Creating blackouts or mass traffic problems.
    c. Hacking into home security systems or appliances.
    d. Hacking into security cameras and altering footage or stealing information about how to access restricted spaces.
2. Fingerprints and Identification
    a. Gaining physical access to restricted areas.
    b. Identity theft via fingerprint authentication or retinal scanners.
3. Virtual Reality
    a. Hacking games or entertainment systems.
    b. Hacking others' vision and misleading them in the physical and virtual worlds.
4. Warfare/Political Action
    a. Hacking planes, drones, helicopters, tanks or other vehicles to shut them down or control them remotely.
    b. Hacking objects on the ground through drones.

you up on your offers (and recently not so many potential breach victims have been accepting the free credit monitoring they have been offered), they still feel listened to, comforted, and thus non-confrontational.

Sometimes your information officers or outside technology consultants will offer to draft the letter to affected customers. And if they do, they may envision it as a form letter, along the lines of many that are already out there. However, allowing them to do so, as opposed to deferring to communications experts (blessed by legal of course) – can rob you of your "goodwill," and turn into one of the worst mistakes leaders can make during a breach.

5. **Crisis plans are necessary, but not sufficient. Sometimes they are dangerous.** The mantra of most organizational crisis and risk managers is to develop a crisis plan. Of course this is a necessary step – you need to lay out the procedures and people to be activated when a breach occurs. You need to think through and articulate your crisis vision and strategy, get the right consultants on tap, have the right technical and communications resources ready to deploy, and

How Hackers Will Use Data in the Future (and the Future is Here) – cont'd

4. Warfare/Political Action (cont'd)
    c. Hacking into fMRIs to change the reports.
    d. Hacking infrastructure.
    e. Hacking missiles and other defense systems.
    f. Hacking navigation systems or classified location information of individuals.
    g. Hacking personnel data (FBI Agents or other covert operatives; government officials; public figures).
    h. Using personnel data or official data to impersonate an official and perform character assassinations or propaganda campaigns with their accounts.
    i. Hacking into security systems of buildings and officials.
5. Cybernetics/Biotechnology
    a. Hacking into prosthetic eyes, hands, or other body parts.
    b. Hacking into a pacemaker or other necessary medical device.
    c. Hacking into cyber brains, controlling people and their bodies against their will.

choose a bulletproof crisis team and team leader that is trusted by the board and executive committee.

However, some crisis plans have the unintended consequence of engendering complacency, especially around cyber crisis. They allow an organization and its leadership to think that everything is handled, when indeed it is not. While no crisis plan can think through every eventuality, its benefit is to focus continual high-powered attention, and prevention, on crisis possibilities and their remediation. Planning can cause an organization to fix a situation or potential breach before a crisis even occurs.

But, there is nothing worse than an outdated plan that has been sitting on the shelf. When a breach does occur, and the team reaches for its "plan," if they find a dusty document that is suited for an earlier reality, they will have to regroup too quickly, and take too much time coming from behind. Sometimes it is almost better to have no plan at all. Unless they are constantly updated and revised, crisis plans can instill a false sense of security.

Our suggestion: the board should insist upon reviewing the plan once a year, seeing a quarterly dashboard of all cyberattacks each quarter, and engaging in a crisis managment "role play" with the crisis team at least every two years.

They should also insist that their CEO play a critical role in every crisis. While he or she does not need to lead the crisis team, with reputations made or broken in a nanosecond through faulty decision making in a crisis, the most senior attention and responsibility is a must.

6. **Key to handling a crisis well is to put together a crisis team that cuts across "silos," puts the right people in charge, and practices robustly and realistically.** The two most important aspects of crisis planning are putting together the right crisis team, comprised of the best thinkers from a variety of departments, and then having them practice realistic scenarios in bi-monthly training sessions.

   So-called "table top" crisis exercises vary widely in quality and effectiveness. We believe that these exercises must be tailored for the individual company and be "ripped from the headlines" to be worthwhile. They also need to be presented in an unfolding dynamic role play, mimicking a real crisis. In this way, the team leader can evaluate each team member's performance, and make sure they are suited to the job.

The ability to think on the fly and under pressure, and to make the exact right decision, in real time, and then express it perfectly in an authentic manner is critical to the task.

7. **Finally, remember that every case is different; be ready to adapt crisis strategies in real time, all the time.** The cyberworld is a dynamic, living environment. Rarely can crisis response and containment procedures be the same from one cyberattack to another. You cannot assume that something you did yesterday (much less what someone else did) will work today, or tomorrow.

   So, be prepared to be constantly on your toes, and to run a marathon at the pace of a sprint.

   If crisis is the new normal, then cyberattacks are the new constant. But public and private response, especially over social media, needs to not only set a new standard for corporate responsibility, it needs to be savvy, smart, and inventive. This new era is going to demand our best and most flexible thinking and response.

About Temin and Company

Temin and Company Incorporated creates, enhances, and saves reputations.

Temin and Company also markets by leveraging the expertise, ideas and insight of its clients to produce differentiated intellectual capital and content.

The firm helps corporations, professional services firms, and other institutions define and strengthen their public image – and their bottom line – through strategic marketing; branding; media relations; thought leadership; social media; speaker, media and leadership coaching; financial communications; and crisis and reputation management.

Strategists, coaches, writers, and social media experts are available “25/8” to assure that every crisis is addressed, and every opportunity leveraged.

Clients include the CEOs and Boards of some of the world’s largest and most well-known corporations, financial institutions, portfolio companies, pharma and biotech companies, law firms, consulting firms, publishing houses, venture capital and private equity firms, authors, politicians, and colleges and universities.