Breaking the Silence

The Sensitive Task of Talking About Cyber Attacks and Network Security Breaches

Companies fear talking about a breach of their computer network almost as much as the breach itself. It's a publicity headache that can make them appear vulnerable or negligent.

But silence is not always the best policy. A spate of recent network breaches shows that companies have a responsibility to tell customers, business partners or investors that sensitive information may have been gleaned as a result of a cyber breach. At that point, companies face a delicate communications task to avoid losing customers, forestall appearances of lax security and governance and maintain business as usual as they try to figure out what happened and how to prevent it in the future.

Moreover, the stakes are higher today as cybercrime has grown more sophisticated in scale and intention. Identity theft is only one objective of cybercrime. Corporate espionage is another. Cyber criminals pilfer intellectual property, pricing data and other competitive information stored on corporate networks. A 2013 Mandiant report on China, for example, found that many attacks of Chinese origin were attempts to steal "intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists."[1]

The issue is causing restlessness in boardrooms. A survey by Corporate Board Member and FTI Consulting found that over half of general counsels and nearly as many directors cited data security as their top legal concern.[2] Those figures nearly double the results from a 2008 survey.

An effective response requires quick action to determine how and when to disclose breaches, how to inform customers and employees, partners and regulators and what information they need to know. Careful sequencing of disclosures and the completeness of disclosures determine how much companies can maintain the confidence and support of stakeholders as they figure out what went wrong, how extensive the damage is are and how best to cauterize the wound.

The Moment of Choice

Deciding when and how to reveal breaches

Given that many attacks go unreported, it is clear that companies exercise wide discretion in determining if, when and what to disclose.

U.S. Securities and Exchange Commission (SEC) guidelines advise U.S. exchange-listed companies to reveal cyber incidents in their financial reports if the event disrupts operations or entails significant costs to increase security or restore reputational damage that will affect financial results.

But short of such clear cut consequences, there is considerable discretion in deciding whether an incident requires public disclosure. The SEC guidelines, for example, may be understood to pertain principally or only to companies for which cyber risks are "among the most significant factors that make an investment in the company speculative or risky." Where that threshold lies is an exercise in judgment.

Practical factors may be more compelling in prompting disclosure than regulatory guidelines. These include:

- Loss or compromise of information that affects relations with a third party, such as a joint venture partner, franchisee, subsidiary, partners within a supply chain or government agencies.
- Loss or compromise of information that affects a large group of individuals. This could include retail customers in a loyalty rewards program, patients in a clinical trial or a company's own employees.
- Loss or compromise of information that can derail projects because it reveals confidential competitive information, such as pricing and other terms of a transaction, expected returns on corporate investments, intellectual property at the heart of a new product, etc.
- A third-party revealing the breach, such as an employee or affected customer posting on a social media site or a regulator in a public disclosure.

Suffering a cyber breach doesn't necessarily indicate an abdication of customers' and clients' trust, but bungling the response does.

[1] "APT1: Exposing One of China's Cyber Espionage Units" published by Mandiant (2013)
[2] "Legal Risks on the Radar" by Corporate Board Member and FTI Consulting, Inc. (2012)

Taking Action and Restoring Trust

Keeping a lid on "downstream" effects

Some of the most pernicious effects of a cyber breach include damage to a company's relationship with its customers, investors, regulators and partners in its supply and distribution chains. Verizon's 2012 "Data Breach Investigations Report," a joint research project involving law enforcement agencies across North America, Europe and Australia, describes significant "downstream effects," such as irate customers and business partners, damage to the corporate brand and heightened regulatory scrutiny. [3]

Factors to consider in diminishing downstream effects include:

- **Timeliness of communications:** Affected parties need to know about a breach within a certain period of time in order to determine the extent to which they are at risk and how they should respond. Timeliness is also critical in telling people what resources a company will make available to help them determine their exposure, find help and protect themselves.
- **Transparency:** Companies need to avoid announcements that raise more questions than they answer. Repeated piecemeal disclosures erode credibility. This requires a careful assessment of how much information to disclose about the source and intention of the breach, the vulnerability that allowed it to happen and whether the threat still exists. Disclosures should provide details on steps the company is taking to determine whether it and its stakeholders are still at risk, if the threat has receded and how it will investigate. It is also important to provide a timeline, however rough and approximate, for future disclosures.
- **Remediation:** A significant part of the disclosure should include the steps that a company is taking to recover from the incident and prevent future breaches. It may well be unclear at the time of the disclosure what next steps a company will take. But affected companies should describe the options they are considering and show that they have given thought to what must be done to remedy the situation, such as whether it intends to engage an outside consultant or law enforcement to assist with an investigation.

An Inside Job?

A critical part of the communication will be determining if and how to address whether the breach resulted from a wholly external source or whether evidence suggests someone on the inside (employees, contractors or others) played a role. This is an extremely delicate task, one with legal implications, and one that defies hard and fast rules.

Internal threats might not be relevant in all cases and it would certainly be misguided to discuss them where they do not apply. It is yet another judgment that companies must make quickly depending on the likely scenarios that may unfold and the questions about internal threats that may arise.

In general, a company should avoid saying anything definitive unless there is strong evidence and a high degree of confidence one way or the other.

However, where it applies, it would be beneficial to state at the outset that the company has ruled out internal sources, provided it is confident in that view. If not, then any communication needs to avoid sparking additional concerns about ongoing threats from internal sources as long as the continuing risk from the inside is deemed to be minimal.

Portraying Control and Responsiveness

The information gathered above will shape all forms of communications: customer letters, customer service scripts, investor announcements, holding statements for media, executive blogs, etc. What's more, it will ultimately shape the narrative that a company is able to portray – either one of control and responsiveness or one of surprise and disarray.

The vigilance and diligence of efforts to protect sensitive information is an obligation to customers and partners, and central to the trust that underlies relationships with them.

Were You Prepared?

Maintaining stakeholders' confidence depends not only how a company responds to a crisis, but also what it was doing to prevent one. An important part of the responsive narrative is to show that data security was a priority. That part of the story will help to stanch criticism of lax standards and governance.

Hence, when disclosing a breach, companies should consider accompanying the announcement with information to show the seriousness that they have historically accorded to cyber security, such as:

- Security policies and procedures that were and are in place.
- Number of full-time security personnel monitoring network and data security.
- Certifications from third-parties attesting to the level of security in place.
- Security staff's participation in or leadership of committees, industry bodies or other working groups dedicated to setting standards and assessing threat levels.
- Internal programs to train staff on the latest cyber security measures and threats.
- Security successes, such as attempted intrusion that they have thwarted. (This is sensitive as it may portray the company as a common target, and hence higher risk for investors, customers and business partners.)

If this information does not accompany public announcements, it will be important to use in preparing Q&As for inquiries from media, regulators and stakeholders (customers, investors, business partners). Again, this too becomes an important part of the narrative that affected companies are able to form.

[3] "2012 DATA BREACH INVESTIGATIONS REPORT" conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit and United States Secret Service

Cooperation with the Government

The heightened level of publicity that cyber breaches attract can draw the attention of regulators or consumer protection agencies. Many forms of data today are "regulated data" – financial records, health records and personally identifiable records. The protection requirements in each of those categories can vary by jurisdiction. A breach will almost invariably raise questions as to whether proper protections were in place prior to any incidents.

Public disclosures should therefore take into consideration how regulators and law enforcement will react. Companies should seek legal counsel to assess the extent of their liability and obligations to inform law enforcement and regulators as well as potential legal recourse if hackers are identified.

Communications plays an important role in this part of the response. Questions about the appropriateness of security infrastructure can be blunted to a certain extent at the outset with clear descriptions of policies and procedures in place to guard against cyber breaches. The more that a company can show the robustness of its security infrastructure and training of its personnel, the better it will be able to blunt criticism, regulatory or otherwise.

In addition, companies should prepare to share publicly relevant information about inquiries from regulators or law enforcement and show cooperation with those bodies. That information can be useful in forming a narrative that demonstrates a sincere desire to inform and assist concerned stakeholders and demonstrate the seriousness with which a company is handling the situation.

Moving On

What is ultimately most important is to show that the company is moving on with business as usual as it investigates the breach and the damage done. It is important to show with each communication that the company is carrying out critical functions and meeting the needs of its customers, suppliers and partners. To the extent possible, companies should reassure customers by saying that product and service delivery will not be disrupted (or if it will, when it will resume) and to reassure investors and business partners by showing that it has retained customers and stanched defections.

Maintaining stakeholders' confidence depends not only how a company responds to a crisis, but also what it was doing to prevent one. This is a crucial part of the response narrative.

Why Wait? Plan Now.

The Law and the Boardroom Study by Corporate Board Member and FTI Consulting found that most companies lack a plan to respond to a serious cyber breach. In addition to the physical IT remediation, the planning process should include protocols for communications. It should also include the creation of a catalogue of activities and procedures that the company can use to show that data integrity and security are top priorities. Creating a track record of aggressive data protection will underscore the company's governance standards and responsibility to its stakeholders.

Showing Regret

Companies need to acknowledge clearly that any incident is an inconvenience first and foremost for customers and business partners. Companies should avoid portraying themselves as victims, and instead underscore their regret for the problems an incident causes others. Wherever possible, they should look for ways to compensate affected parties.

The vigilance and diligence of efforts to protect sensitive information is an obligation to customers and partners, and central to the trust that underlies relationships with them. Suffering a cyber breach doesn't necessarily indicate an abdication of that trust, but bungling the response does.

Daniel Del'Re
Director
+852 3768 4547
daniel.delre@fticonsulting.com

CRITICAL THINKING
AT THE CRITICAL TIME™

About FTI Consulting

FTI Consulting, Inc. is a global business advisory firm dedicated to helping organisations protect and enhance enterprise value in an increasingly complex legal, regulatory and economic environment. FTI Consulting professionals, who are located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges in areas such as investigations, litigation, mergers and acquisitions, regulatory issues, reputation management and restructuring.

www.fticonsulting.com