

*Cyber crisis management:  
A bold approach to a bold  
and shadowy nemesis*

August 2011



---

## ***Table of contents***

---

***The heart of the matter*** **2**

***Cyber crisis management:  
A new philosophy and approach to  
incident response***

---

***An in-depth discussion*** **4**

***A roadmap to data breach survival***

Bringing clarity to chaos

Walking bravely through the cyber threat landscape

Defining cyber crisis management

Developing a cyber crisis management solution

Critical success factors in responding to cyber crisis incidents

---

***What this means for your business*** **16**

***Taking a stronger, broader, and bolder approach  
to managing cyber incidents***

---

*The heart of the matter*

Cyber crisis management:  
A new philosophy and  
approach to incident  
response

*“[T]he great test lies not in the crisis itself but in the ways we respond.” Steve Forbes, Forward in The Communicators: Leadership in the Age of Crisis*

### **Keeping up with the cyber cabal to keep your business safe and sound**

“Everybody... has to be prepared to be hacked.”<sup>1</sup>

As cybercrime runs rampant, reports of major cyber incidents and data breaches that would have been unimaginable just a few years ago pour from today’s headlines, wreaking havoc on organizations of every stripe. According to one senior government official at the Department of Homeland Security, “[s]ensitive information is routinely stolen from both government and private sector networks.”<sup>2</sup> And the cost of information security breaches continues to rise. In 2010, such breaches cost companies an average \$7.2 million per incident.<sup>3</sup>

These breaches can have a significant, potentially devastating effect on a company’s reputation or financial position. Yet too many organizations continue to treat these breaches as technical problems that require technical solutions.

All the while, the cyber threat landscape continues to breed an increasingly sophisticated underworld of criminals who act upon a variety of motives to compromise their many targets. This cyber cabal includes:

- Loosely organized hacktivist groups—hacking activists—that steal and disclose confidential information and damage the company’s reputation.
- State-sponsored groups that steal economic intelligence for competitive advantage.
- Organized crime groups that steal sensitive customer data and trade it in the criminal underground for financial gain.

These advanced groups gain broad access to an organization’s computer systems and networks and are able to maintain that access for days, months, and sometimes years, causing continuous damage. Companies that detect these cybercrimes (or, more typically, those who are notified of the crime by law enforcement or another third party) are often quick to focus on the technical aspects of the breach. As a result, the initial—sometimes only

—step a compromised organization takes is to launch an internal investigation using the organization’s IT operations department. Typically, this team tries to quickly determine the source of the attack (if possible), plug the hole with a technical fix, and assure management that the problem is solved.

Yet all too often, the problem is not solved and the company remains significantly exposed to operational, financial, and litigation risks. Granted, not every cyber incident results in a far-reaching compromise of systems or disclosure of sensitive, confidential information. But over time, it’s quite likely that one of these incidents will erupt into a major, high-profile cyber event.

Companies need to remain prepared for such cyber crises. This entails not only creating—and testing—an incident response plan, but also establishing the capability to respond to a significant cyber event with a cyber crisis management solution. Indeed, the cyber crisis management solution can be your organization’s key to data breach security and survival.

Read on to learn more about how you can ensure that your business is well equipped to survive a cyber security incident or data breach of sensitive information by applying a new approach to cyber threat management that’s founded on the realities of the evolving cyber threat landscape.

1 Mr. Gordon Snow, Assistant Director, FBI Cyber Division, “The 21st Century Cyber Threat,” CyberFutures Conference, National Harbor, Maryland, 31 March 2011.

2 Testimony of Deputy Under Secretary Philip Reiter, National Protection and Programs Directorate, Before the United States House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, “Examining the Cyber Threat to Critical Infrastructure and the American Economy” Release Date: March 16, 2011.

3 2010 Annual Study: U.S. Cost of a Data Breach, Ponemon Institute, March 2011.

---

*An in-depth discussion*

# A roadmap to data breach survival

## Bringing clarity to chaos

### You made it to Congress!

#### Now what?

As in any crisis situation, companies ensnared in a cyber incident are trying to operate in the throes of chaos. Cyber incidents often trigger internal or external forensic cyber investigations, an especially messy undertaking. The details of how the compromise occurred, whether and how much data was removed from the environment, and whether the cyber attack is ongoing are likely to fluctuate throughout the ordeal.

In our experience, when cases involve unauthorized access of customer information, the number of customer records confirmed as stolen will vary dramatically from the initial estimate and from estimates at several points throughout the investigation. Still,

businesses can bring order to this crisis environment and lay the foundation for a structured, disciplined response to the breach. Indeed, it's this structure and order that will ensure that the victim organization is well positioned to face any future litigation or regulatory or Congressional inquiry.

Over the past decade, data breaches and cyber intrusions have increasingly resulted in Congressional inquiry and follow-on Congressional hearings. Some companies appear to survive these inquiries relatively unscathed, but others respond in a way that opens the door to further criticism of their handling of the incident. Often, the outcome depends not on the number of records compromised or the nature and scope of the intrusion, but rather on the extent to which the organization can demonstrate a structured and orderly handling of the cyber event.

To cultivate an environment in which a structured, orderly response will shine through in the event of a cyber breach and ensuing inquiry, organizations should strive to incorporate these major elements of a cyber crisis response life cycle. Shown in Figure 1.

**Figure 1: Key elements of a structured and orderly cyber crisis response**



Num	Phase	Description
1	Information security program	Company X has a robust information security program that conforms to internationally recognized data security standards. The program is certified against these standards; and obtaining such certification requires validation from independent third-party auditors.
2	Cyber event detection	The information security program identified and detected the cyber event in question. (Alternatively, if a third party such as law enforcement notifies the organization of the attack, you hope to be in a position to state that the attack was sophisticated, targeted, and is known to have occurred undetected in many organizations despite robust information security programs.)
3	Incident response	Detection of the cyber event triggered the organization's incident response program, which is composed of both an incident response plan and formation of an internal response team to coordinate the response.
4	Internal investigation	The organization immediately launched an internal investigation.
5	Third-party forensic investigation	The internal investigation triggered a forensic investigation in which outside experts were contacted and retained within 24 hours.
6	Contact law enforcement	The organization contacted law enforcement immediately after the forensic investigation commenced.
7	Customer notification	Customer notification was made as soon as the forensic investigation confirmed the scope and nature of the attack, including whether customer information was involved in the intrusion.
8	Containment & remediation plan	The organization was able to quickly establish and implement a containment and remediation plan.

## How can your organization adopt a structured, orderly cyber crisis response?

A response to a Congressional inquiry evolving from this model will likely convey that the organization was in control of the crisis and the event, rather than subject to the chaotic events unfolding in the wake of the attack. Otherwise, the organization can appear to be entirely reactive to the circumstances at hand and utterly immersed in an out-of-control, chaotic environment. This is the likely outcome if your response merely presents a chronological timeline of the events in the incident response process, with each hour and day requiring the engagement of multiple vendors and approaches, depending on which facts surfaced.

How can your organization adopt a structured, orderly cyber crisis response? A cyber crisis management program can enable your organization to build clarity and discipline out of a chaotic environment and, ultimately, survive the data breach with minimal damage—with the added benefit that should you be hauled into court or face a Congressional hearing, you'll be poised to demonstrate to lawmakers a comprehensive approach that has been outlined proactively.

### **Walking bravely through the cyber threat landscape**

The cyber threat landscape continues to breed new, advanced groups capable of targeting and successfully compromising any organization they set their sights on. This cyber crime cabal has global membership and extreme patience; it's also highly organized and motivated, sometimes well-funded, and fully immersed in its tradecraft. Examples include:

- **Hactivists:** loosely organized and affiliated groups of politically motivated hackers
- **Organized criminal groups:** loosely organized global hacker groups composed of traditional organized crime groups
- **State-sponsored groups:** sophisticated and well-funded hacking groups sponsored by foreign governments

Each of these offenders is motivated by one or more of these goals:

- Significant disruption of business operations
- Leaking sensitive corporate information to the public to damage a company's reputation

- Leaking sensitive customer information to the public for financial gain or to harm the organization
- Obtaining sensitive economic intelligence for a competitive advantage
- Obtaining and maintaining control of critical US infrastructures
- Maintaining remote access to systems for a long time to re-compromise networks
- Stealing personal customer data, including card data and identity information, to resell in the criminal underground for financial gain
- Stealing sensitive corporate information for profit, including extortion

Clearly, we've entered a new era of cybercrime that's based on advanced groups capable of targeted, well-orchestrated, sophisticated, prolonged, repeat attacks on businesses. This era is a world apart from the prototype attack of a decade ago, in which a solo hacker engaged in a one-time offense on a system for intellectual curiosity or just for fun. This new era cries out for a new incident response approach. Are you listening?

**Defining cyber crisis management: Incident response is more than a technical problem with a technical solution**

Traditionally, companies facing a cyber incident, such as a denial of service attack on their network, have treated the breach as a technical problem and responded with a technical response (e.g., by implementing anti-DDOS measures or otherwise increasing security perimeter controls). Two factors have changed this landscape, rendering

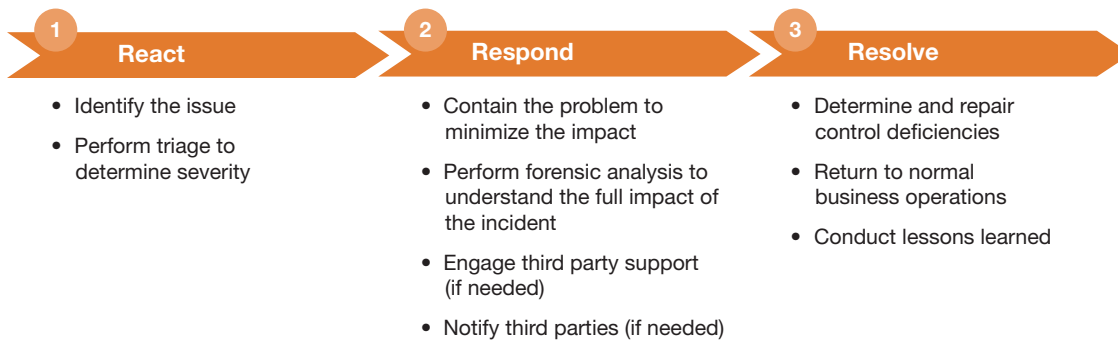
these incidents as far more serious and raising the stakes on how companies respond: (1) the scope and nature of the attacks and (2) the amount of publicity surrounding these events.

This is no longer about a solo hacker who compromises systems when the batteries run out on some other diversion. Today's cyber threat groups are advanced, sophisticated, and able to gain deep and prolonged access to systems and networks, where they can cause sustained damage over time. Media attention to these events

has increased along with the threats they pose, especially with respect to publicity-hungry political hactivists.

Given these factors, companies facing a cyber incident will encounter peril if they assume that a particular incident is a one-time manifestation of a technical problem that can be solved with a technical solution. Significant security incidents will require an entire cyber crisis management solution across the cyber incident response life cycle, from react, to respond, to resolve. Shown in Figure 2.

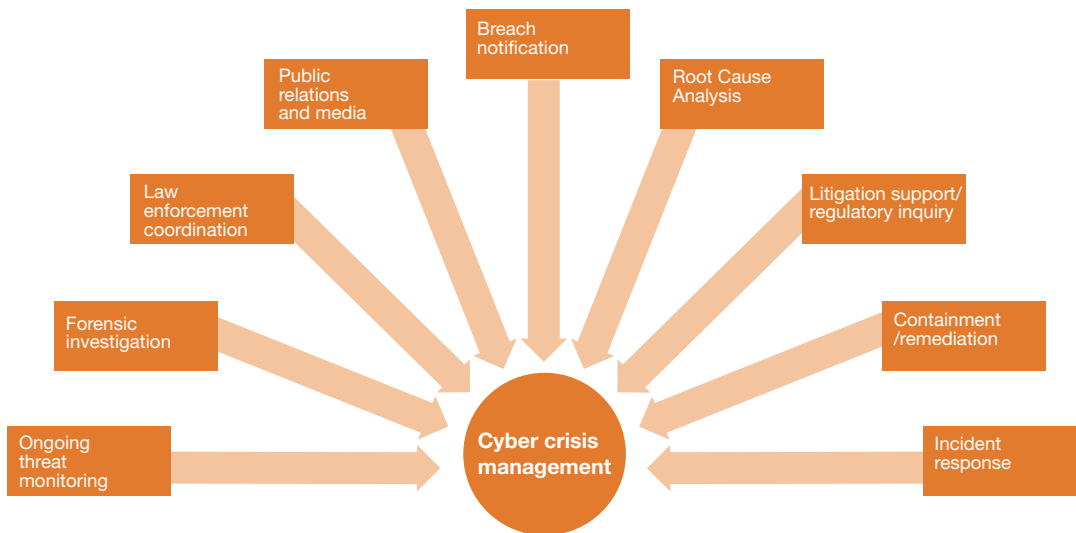
**Figure 2: Cyber incident response process**



During any or all of these stages in the cyber incident response process, the company may need to perform, or have performed, any number of discrete services or actions, only some of which require technical resources. For example, in the react stage, in order to perform triage to determine the severity of the incident, an organization may need to engage in ongoing threat monitoring of the criminal underground to assess the

extent to which criminals plan to continue attacks on the company's systems. In the respond stage, the targeted company may need breach notification services to prepare and distribute letters for customers affected by the breach. Finally, in the resolve stage, the company may need to develop and implement a remediation plan to ensure that security vulnerabilities are properly repaired against future attacks. Shown in Figure 3.

**Figure 3: Cyber crisis management model**



## *Your organization may have internal capabilities to carry out some of these actions*

Your organization may have internal capabilities to carry out some of these actions; however, most organizations will lack the expertise and resources to carry out many of the discrete tasks, and will need to bring in any number of external parties. In our experience, services requiring outside specialists include:

- **Threat support analysis services** monitor the criminal underground and analyze the extent to which the attack may be ongoing against the victim's systems and network.
- **Incident response teams** provide cyber investigative human and technical resources, incident management, investigation and containment support, and remediation of security control weaknesses.
- **Forensic investigation services** efficiently secure and analyze compromised systems and electronic information. These services can include forensic preservation and analysis of computer systems, live memory, malicious software (malware), network traffic, and monitoring logs (firewall, IDS/IPS, proxy, DNS, A/V, etc.).
- **Sensitive data discovery services** identify sensitive data in structured and unstructured database environments, as well as identify instances of data leakage involving intellectual property and trade secrets.
- **Advanced network analysis and breach indicator services** identify evidence that may indicate a past breach or a compromise in progress. These services often involve investigation of network traffic and critical data stores for breach indicators and internal and Internet-based penetration testing.
- **Customer notification, mailing services**, and call center support provide a full array of customer care services in the event the compromise involves personally identifiable information and triggers requirements under state and federal data breach notification laws.
- **Fraud mitigation services** provide credit monitoring solutions to customers whose personal information was compromised as a result of the incident.
- **Public relations services** assist with the rapid development and deployment of a public relations and communications strategy at the forefront of a crisis.

As a result of the need to bring in any number of external parties to perform various functions, responding to significant security incidents can quickly become a 'soup of vendors' conducting sometimes overlapping and often uncoordinated data breach response services.

*A cyber crisis management team can manage all the moving parts of a crisis response.*

**Developing a cyber crisis management solution**

A cyber crisis management solution can help you recognize the inefficiencies of an uncoordinated incident response process that relies on independently operation parties who are performing discrete services toward a common goal. A cyber crisis management team can manage all the moving parts of a crisis response (separate from but closely aligned with the more narrowly focused internal cyber incident response team).

The core incident response team is composed of a technical investigative team of technical subject matter specialists. Moving upward, the team broadens to include an incident team leader and others less involved in the daily technical response. Moving upward again, the broader core team will ultimately include non-IT management stakeholders from legal, finance, and other senior executives. Shown in Figure 4.

**Figure 4: Cyber incident management team**

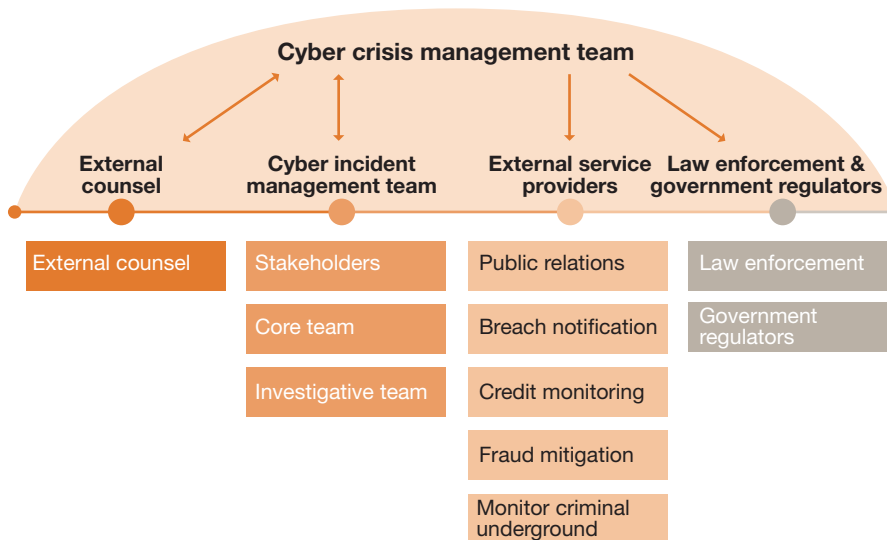


What's missing from this picture, however, is a coordinated crisis management approach that ensures a structured and orderly response of: (1) all services provided in responding to the significant cyber event, including, for example, services related to public relations, breach notification, and fraud mitigation, and the monitoring of the external criminal underground for information indicating a continuing attack; and (2) all messaging and communications with outside parties, including the broader public, customers, regulators, and law enforcement. Who is ensuring that each of these parties is properly

coordinated and working toward a common goal? Who is ensuring coordinated and consistent messaging to external parties? Shown in Figure 5.

The cyber crisis management team should act as the program management office, or liaison, between the internal incident response team and the broader environment that includes an array of internal and external groups, ensuring the proper coordination among the players. Ultimately, it's this team that will lead the organization into a structured and orderly cyber crisis management response to the security incident.

**Figure 5: Cyber crisis management model**



## **Critical success factors in responding to cyber crisis incidents**

In addition to the development of a cyber crisis management solution, your organization's approach to responding to security incidents should incorporate a number of critical success factors. As in any crisis situation, the first 48 hours after a compromise is detected, followed closely by a consistent approach over the next several weeks, is critical in determining whether your organization will weather the storm or go down in flames. From our experience in observing and assisting businesses in the wake of a cyber crisis, we've identified several critical elements:

### **Your communications strategy is central to the mission.**

In recent years, cyber crisis incidents are becoming increasingly visible events receiving considerable media attention. You should expect that the details of your cyber crisis event will quickly appear in major news outlets. This 'media frenzy' is the result of two factors.

First, we've seen a resurgence of hackers: hacking activists. Often, the sole purpose of these hackers' criminal pursuits is to expose information belonging to, or concerning, the victim organization. These criminals play in the media space, strongly influence the dialogue, and are masters at using the media to achieve their political goals.

Second, we've seen an increasing number of available media outlets (e.g., Twitter, blogs, social media) to enable these criminals to quickly disseminate their ill-gotten gains. These first lines of media exposure often directly feed into major news outlets. It's become increasingly common to see hackers post confidential information and details of a data breach to a website that's closely tracked by journalists writing for major newspapers and magazines. As a result, your cyber crisis management solution must fully reflect the crucial media component in the incident response process. Indeed, the media space is becoming the new courtroom battle. Here are some crucial elements your approach should include:

- **Incorporate and integrate.** Incorporate a public relations strategy and communications plan into the cyber crisis management solution and integrate the public relations group with the crisis management team.
- **Plan ahead.** A communications plan is a key element of an effective crisis management response. Indeed, the absence of a plan makes it difficult to have an effective response. A communications plan that's deployed early in the process can assist with a coordinated and effective fact-gathering investigation, effective media statements and strategic regulatory outreach, and even the identification of litigation positions.

- **Control the narrative.** Use various media tools to take in information in real-time, push out information at strategic times, and gain a voice in the media space. Ensure that your content is succinct, precise, and delivered consistently across your organization.
- **Be decisive.** Pure crisis often calls for pure action. Understand that in crisis situations, decisions often must be made based on imprecise information. This understanding will help you avoid the trap of remaining stagnant while waiting for precise information amid a crisis.

Each of these elements will significantly help your organization bring an effective public relations component to bear in positioning your entity appropriately with the media and the public.

*Cyber incidents, especially those involving the compromise of customer data, open the company to litigation or regulatory investigations or inquiries.*

**Establish a point of contact to act as a secretary.**

Almost certainly, cyber incidents, especially those involving the compromise of customer data, open the company to litigation or regulatory investigations or inquiries. Assume that your organization's decisions in responding to the cyber incident will be challenged in litigation or questioned in regulator or Congressional inquiry. The availability of detailed notes will assist business leaders in recalling key facts about the key junctures when critical decisions were made along the way (for example, whether to notify customers or delay customer notification, whether to reach out to law enforcement, and whether to hire outside consultants or handle the matter internally).

It's therefore critical to document your organization's decision-making process with extreme detail and accuracy when caught up in the midst of a cyber crisis. At the outset, you should appoint a go-to person involved in the process to take detailed notes on every call in every meeting. This will help tremendously in creating a written chronological investigation report, whether for internal purposes or to share externally.

**Don't notify customers until you have all the information. Facts continues to surface.**

The decision regarding when to notify customers, if the facts warrant, will likely be the most thorny and contentious of decisions during a cyber crisis incident. Experienced data breach responders will agree that most often the key business leaders will push, and push hard, to notify customers as quickly as possible once even a scintilla of evidence of data compromise emerges. These are the customers with whom they have developed a trusted relationship, after all, and without customers, the business fails. In the business leader's eyes, the customer needs to be informed sooner rather than later of any indication that his or her personal information might have been compromised. It's certainly a logical reaction.

In our experience, however, the only thing worse than having to notifying customers of a potential data compromise is having to notify them a second time. Undoubtedly, the second notification is far worse than the first, not only because it often contains a number of compromised records that exceeds the number disclosed in the first round, but also because any customer trust that remained after the first notification has now completely and forever disappeared.

Therefore, don't notify prematurely. Remember that cyber forensic investigations are messy. Until the investigation is over, these facts are likely to be in a constant state of flux: how the compromise occurred, whether and how much data was removed from the environment, and whether the cyber attack is ongoing. Your organization needs to be comfortable that you're at a place where the facts are solid and that re-compromise is unlikely. Ensure that the incident responders have double- and triple-checked the facts and that the facts have been confirmed by an independent reviewer. Ensure that the right questions have been asked and that the proper time and resources have been given to investigators. You want to notify only once and you want those facts to be correct.

*Your organization needs to be comfortable that you're at a place where the facts are solid and that re-compromise is unlikely.*

**Activate your incident response program immediately after the incident is detected.**

The incident response program is the underpinning that will introduce order internally and externally to the chaotic environment in the wake of a cyber incident. The program should consist of both a written plan that has been tested and the formation of an internal response team (discussed in more detail later). Of course, if your organization doesn't have a plan, it needs to develop one. If your organization has a plan that was developed in prior years solely for physical compromises or non-cyber emergencies, it's important to revise, enhance, or review it for relevancy in this more challenging information age.

Just as critical to developing a security incident response plan is the need to test it through threat modeling, scenario planning, and tabletop exercises. These exercises often consist of presenting a brief cyber incident scenario to key leadership and members of an incident response team, followed by a series of questions to key leadership on how they would respond to the scenario. Their responses help identify weaknesses in the incident response process and

test organizational effectiveness in managing critical events. These exercises should be geared not only toward a technical response (i.e., How would we fix this system?), but also toward the larger incidents that should trigger a cyber crisis management response (i.e., How would the organization respond to prime-time television coverage of the event?). The exercises often result in recommendations in the form of an after-action report.

**The incident response program should trigger formation of an incident response team.**

The incident response team is an internal team that will coordinate the management of and response to the particular incident. This overall team will include several components, including an investigation team and key management stakeholders. Some individuals may overlap from one component to another. The team should have one designated point of contact responsible for the entire cyber crisis management response who will also act as the leader of the cyber crisis management team.

**Hire outside counsel with extensive experience in data breach response.**

Just as complex, structured transactions that carry significant tax ramifications require legal counsel with tax expertise, cyber incident response requires specialized legal assistance with extensive experience in data breach management and response. Specialized data breach and crisis management attorneys can assist in the interpretation of the patchwork of state and federal laws that will govern the incident response approach. Such counsel will also provide guidance about initial regulatory notifications and assess whether NYSE/Nasdaq and SEC disclosure requirements are necessary.

This expertise should also include the ability to establish a workable law enforcement approach that protects the company while responding to law enforcement requests in a timely manner. In the event that law enforcement is not aware of or pursuing an investigation into the cyber incident, counsel (and other experts) can walk your organization through the advantages and disadvantages of reporting the incident to law enforcement and guiding you to the appropriate entity within law enforcement.

Experienced outside counsel will also understand the significance of your organization's burden as a cybercrime victim and the importance of positioning your organization as such. Counsel will be able to review the legal remedies available to your organization as a crime victim. For example, while the Computer Fraud and Abuse Act (Title 18, United States Code, Section 1030) is well known for its use in prosecuting perpetrators of hacking crimes, a key civil provision was added in 1996 that affords certain rights to victims of computer intrusions. In particular, Section (g) provides that an individual who suffers damage or loss as a result of a violation of the Act "may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."

The injunctive provisions of this section assist a victim in retrieving stolen data as the result of a system compromise and preventing its dissemination. For example, employers can use this section to obtain injunction relief against former employees who improperly access the employer's computer system and gain access to information that may be used to compete against the employer. Experienced outside counsel can make the company aware of the legal rights afforded to crime victims so business leaders can act on them under the appropriate circumstances.

**Establish the cyber crisis management point of contact to quickly identify and efficiently manage all outside resources.**

Cyber incidents often call for myriad other experienced outside resources. As outlined earlier, many kinds of services may require outside resources in a cyber crisis incident. Your organization does not want to be in the position of hiring a new vendor each time the facts of the investigation change, or of relying on overlapping responsibilities and uncoordinated efforts. Establishing a cyber crisis management point of contact to quickly identify and efficiently manage all outside (and inside, to some extent) resources is critical to a smooth and structured cyber crisis response. The point of contact can be internal to your organization or a trusted outside advisor; however, the person must at a minimum have deep knowledge of technical responses to complex investigations and familiarity with crisis response from a communications perspective. In addition, the point of contact is responsible for setting up a crisis team, deciding on additional resources, and coordinating a structured and orderly cyber crisis response.

---

*What this means for your business*

Taking a stronger,  
broader, and bolder  
approach to managing  
cyber incidents

The cyber threat landscape continues to breed new, advanced cyber cabals capable of targeting and successfully compromising any organization. These sophisticated, highly motivated groups gain broad access to the company's computer systems and networks and are able to maintain that access for days, months, and sometimes years, causing continuous damage. In responding to these cyber incidents—if, indeed, they are detected—companies often take an overly technical approach, and, in doing so, leave the company significantly exposed to operational, financial, and litigation risks.

Organizations need to ensure that they're well-prepared to survive a cyber security breach by applying a new approach to managing these incidents. The response to today's breed of cyber crime should reflect the realities of the evolving cyber threat landscape and

embrace the establishment of a cyber crisis management solution. In the persistent war for cyber security, brand integrity, customer loyalty, and fiscal viability, a structured, orderly, and coordinated response to cyber crisis can mean the difference between cyber breach and cyber peace; either way, the outcome will likely have long-term implications for your business.

A well-planned and efficiently executed cyber crisis management solution can serve as your organization's ticket to data breach survival—despite the shadowy threats today's cyber cabal might plan and dare to launch. Their sophistication continues to evolve. And yours should, too.

***To have a deeper conversation about how this subject may affect your business, please contact:***

David Burg  
Principal  
PwC  
(703) 918-1067  
[david.b.burg@us.pwc.com](mailto:david.b.burg@us.pwc.com)

Ed Gibson  
Director  
PwC  
(703) 918-3550  
[ed.gibson@us.pwc.com](mailto:ed.gibson@us.pwc.com)

Kimberly Peretti  
Director  
PwC  
(703) 918-1500  
[kimberly.k.peretti@us.pwc.com](mailto:kimberly.k.peretti@us.pwc.com)

Tomas Castrejon  
Director  
PwC  
(415) 498-8418  
[tomas.m.castrejon@us.pwc.com](mailto:tomas.m.castrejon@us.pwc.com)

Shane Sims  
Director  
PwC  
(703) 918-6219  
[shane.sims@us.pwc.com](mailto:shane.sims@us.pwc.com)

David Nardoni  
Director  
PwC  
(213) 356-6308  
[david.nardoni@us.pwc.com](mailto:david.nardoni@us.pwc.com)