Cyber Crime:

Is Your Company A Potential Target?

Are You Prepared?

By ALBERT J. MARCELLA, Jr., Ph.D., CDP, CFSA, CISA

Ian I. Mitroff, professor of business policy at the Marshall School of Business at the University of Southern California, said in a recent interview, "Corporations – or IT departments – tend to focus on crises they know about. That doesn't serve them well. It's not the crisis you know that will kill you; it's the one you don't know. There are all sorts of crises: economic, reputational, human resources. Organizations are susceptible to a wider array of crises than 30 years ago, and any one can be the cause or the effect of any other. Something in IT could trigger something elsewhere, or vice versa. Crises don't give a damn about the silos and walls we set up."

Unfortunately, Professor Mitroff's warning may well go unheeded, if senior management fails to listen and to listen well. If the corporate audit function is truly to serve and to represent management as its "eyes and ears" then it becomes the duty of the audit function to look at this world through different lenses. You have to ask the questions no one would think of asking, even when those around you may scoff at your particular view of the world. For if those of us tasked with assessing the security and controls within organizations do not ask these questions, or do not have this view, who will?

Given the ever increasing demands being placed on information technology and the infrastructures supported by those technologies throughout an organization, examining the organization's preparedness to effectively respond to various and diverse "crisis events" should be an objective incorporated into the very charter of the audit function. Who within your organization is responsible for assessing the organization's crisis management capabilities? Does your organization even have a crisis management effort, department or team? Who manages this critical function? Does responsibility for such a critical function fall to the already overburdened "security" department, IT department, business continuity planning team? Who?

Proactive organizations have vision and prepare for crises which have yet to happen. Reactive organizations unfortunately only prepare after the crisis has disrupted operations or worse, caused a loss of life. Is your organization proactive? Reactive?

Technical people tend to think in nice, neat boxes. In a company that is proactive, when you look at how crises happen, you realize that human beings operate technology. You look at how people make errors, how the best-laid security plans can be breached by error or omission or commission. You dialogue with other parts of the company to see how IT connects, how someone could get in even with the best of security. When you have an internal crisis team, you use a mix of people – not just IT people in isolation. A mixed group comes up with richer scenarios. You don't start with the assumption that it can't happen. You say, "This has happened," and work backward to find out how it could happen.

Crisis Management Case Study

The following crisis management case study was first used during a recent seminar presentation on cyber terrorism, conducted by the author. When asked to develop a response, given the parameters of the case, most attendees were unable to provide a plausible course of action if the event took place within their own organization. Many

simply sat in disbelief that such an event could potentially occur within their organization. Unfortunately, such an event can occur. The amazing thing is that it hasn't occurred already. Or has it?

Upon further examination of various system constraints and environmental considerations, it became critically clear how probable the crisis event could actually be. This scenario, or one very much like it, would have a direct impact (with varying degrees of collateral damage) on any reactive organization.

It cannot be stated with any degree of certainty, that such a scenario has not already taken place. Many organizations would be reluctant to publicly reveal the details of exposures and breeches to their internal systems and organizational infrastructure.

Cyber Coercion

The exposure represented by the specific threat of criminal coercion to corporate personnel and infrastructure, should not be taken lightly or ignored. Such coercion can be justifiably considered and treated as a crisis event. The conditions leading to the coercion of an employee can vary greatly. It is critical that organizations have in place, procedures to routinely conduct background investigations of all employees, especially those employees who have access to sensitive and critical information technology and technology infrastructures.

Does your organization conduct unannounced, random background investigations of employees with access to sensitive and critical organizational information and information systems? Why not? Should such investigations be made part of a condition for continued employment? What would be the impact to the organization should an employee with access to truly sensitive corporate data, disclose that data to unauthorized persons? Could periodic background investigations potentially reveal a "liability" or exposure in a person's background, which if left unaddressed could pose a threat to the organization or its personnel?

Professor Mitroff, in further discussions relating to crisis management, suggested employing "internal assassins," IT people who would concoct a scenario that would do the most damage and take the longest time to find out. They might also look at how someone with a high school education versus a Ph.D. could sabotage you. Then what would you do to blunt it? How could you know this is beginning to happen? What is in your organization, culture, reward-and-punishment system that would make someone disgruntled enough to do this?

Auditors and associated security professionals may see this as taking security measures to the extreme. However, the tactic has merit. Assessing the weaknesses within a specific environment may require the assessor to take unconventional measures, approach the evaluation from different perspectives and points of view, and to think, with the same mindset, as the cyber criminal/terrorist might think. Are you thinking like a criminal? If not, you better start.

Threat Evaluation

Coercion means to compel someone by force or actions to do something which they would not, as a rule, consider doing under normal conditions. The coercion itself does not necessarily have to be physical or be restricted by physical or geographical constraints.

Coercion is such an ambiguous word, conjuring up all types of unsavory images as well as psychological implications. In this case study, the perpetrator's motive is not necessarily clear. The motive could be to create a disruption to customer service and normal company operations. This is simple intimidation, an attempt to incite a loss of customer confidence toward or to generate financial instability within the targeted organization. Athough, it could be more personally motivated, such as in a vendetta against an employee or the organization itself?

The following case study is intended to ask many more questions than it is designed to answer. Its objective is to raise the reader's level of awareness and to stimulate creative thinking. If the case study motivates just one reader to reassess his/her organization's level of crisis management preparedness and the organization's ability to respond to a crisis event, to move from a reactive posture to a proactive one, then this case study has accomplished its objective.

The very real situation presented here is but one of a multitude of crisis events that may befall any organization. Is your organization prepared? Would your organization be able to cope? Respond? Continue ongoing operations? Provide for the safety of its personnel and those who depend on your organization, domestically and globally? Is your organization reactive or proactive?

Additionally, the crisis event presented in this case raises questions, which require answers that are clear, informative, decisive, and immediate. Failure to have a proactive and tested response plan to a crisis event (general or specific) in place could result in the financial collapse of the organization or worse, injury or death to company personnel.

Think you've seen it all? Think you're prepared? Think again … .

Cyber Crime: A Case Study

Your organization's network administrator has just returned from lunch to find an addressed manila envelope on his/her desk. Opening the envelope he/she finds the following contents:

- ❑ A CD.
- ❑ A note which simply reads: Upload this CD's contents to your organization's central server by 3 p.m.
- ❑ A typed sheet of paper, which details in chronological order, the activities of your network administrator's family from the previous weekend.
- ❑ Photographs of each member of the network administrator's immediate family cross referenced to the chronological activity list.
- ❑ Photographs of the network administrator's parents, dated today, who are living in another state, photographed outside their home.

It is now 1:30 p.m.

1. How would your network administrator react? What does your network administrator do?
2. Does your organization have in place, a response plan to deal with this type of cyber terrorism? Has this been considered a realistic scenario in your organization's disaster recovery and business continuity plan? Why not?
3. Does the network administrator know whom to call first? His/her family? His/her parents? The local police? Federal law enforcement? Company security personnel? Who? Should he/she call anyone at all?
4. Do local authorities know how to respond or react to an IT "crisis event" such as this without jeopardizing all parties involved? Does your organization's in-house security (IT as well as physical security staff) know how to react and respond?

It is now 2 p.m.

5. Will contacting any of these parties tip off the cyber criminal, potentially resulting in the loss of life? Destruction of corporate assets (buildings, inventory, foreign operation locations)? Will it result in a retaliatory strike on the organization's physical plant or general personnel population? Locally? Regionally? In a foreign country?
6. Does your organization have the ability to replicate its network and run the CD, to ascertain what potential damage (if any) might occur by uploading the CD as instructed?
7. Does the organization have the ability to "port" this shadow network out as the "real thing" so as not to jeopardize the intended cyber target yet seemingly to comply with the criminal's demands? Is this even a wise and logical philosophy given what is at stake?
8. Do internal controls exist within your organization's network environment, which could neutralize the affect of malicious code being directly uploaded to the network's central server?
9. Does your organization have the ability to compartmentalize sensitive company data so it remains secure in the event of a system-wide exposure incident?

It is now 2:20 p.m.

10. Can your organization ensure that company confidential data is not accidentally disclosed to third parties who may be called in to assist? To those who may be given remote access to your system? Or who may ask (even demand) to have access to your network to track and/or monitor the result of uploading the contents of the CD?
11. What procedures are in place to evacuate the location should the criminal target physical plant facilities, as a failure to comply with his/her/their demands? How will this be accomplished without tipping off the criminal (who may be observing operations from a secure location)? Without panicking employees?

It is now 2:45 p.m.

12. Who in your organization is responsible for leading, coordinating, and assuming command and control in such an event?
13. Who is responsible for dealing with the now (presumably) distraught network administrator who, when attempting to call, cannot reach his/her family or parents? Who allowed the network administrator to make such an outgoing call to begin with? Could such action(s) compromise the situation even further?
14. Does your organization have a plan in place to notify all significant customers and end users (civilian, military, corporate, etc.) that

may depend on your network, of its impending unavailability; should it be shut down or rendered useless? How is this accomplished without (a) panicking said users, (b) disclosing sensitive operations information, (c) exposing the organization to unforeseen liabilities?

15. Does your organization have a legal requirement to notify external third-parties of an impending network "shutdown/problem" (e.g., SEC, Federal Reserve Board, FCC, FTC, etc.)?
16. What is (or will be) the financial impact to your organization due to a wholesale corruption of its network and related IT operations? Legal implications? Customer confidence implications? Market implications?
17. How does your organization plan to "contain" the current situation (i.e., preventing anyone from leaking the current crisis situation to external media sources)?
18. How do you determine the threat is actually genuine and not a hoax?

It is now 2:55 p.m.

19. How quickly can you move critical network dependent applications and services to an alternate server/vendor/site? How do you determine which applications and services are "critical?" How do you know that the cyber criminal doesn't already know whom your organization uses for business continuity/disaster recovery services, and has potentially compromised that system (or vendor's operations) as well?
20. Does the network administrator even bother to call or tell anyone about the note and CD?

Reacting simply out of fear for his/her family and with no previous training/exposure to such a possibility simply follows the directions given on the note and then leaves the building.

BANG – it is 3 p.m.

Time is up. What are you going to do?

Conclusion

The world has changed in the past 24 months in ways no one could have imagined. Constructing challenging and creative crisis/threat scenarios should no longer be considered optional but should be part of every organization's aggressive and proactive, ongoing continuity planning strategy.

What is the probability of a crisis event, as described above, occurring within your organization? Low? Unrealistic? Credible? Don't know? A crisis event of some magnitude is virtually guaranteed to happen. The only question is when and how.

❑ Did you have solid answers to these very critical, operational questions? How long will it take your organization to develop realistic, credible answers?

❑ Is your organization prepared to respond to a similar crisis event?

❑ Has your organization tested its preparedness to manage a crisis event such as this one? Does it have any plans to do so? To do so on a regular basis?

❑ Are threat or crisis events such as the one above regularly addressed as part of your organization's business continuity planning process? Why not?

❑ Has this case study been shared with all responsible recovery and security team personnel?

Are you willing to bet your organization's financial security, its future and the safety of its employees on probability tables?

If not, then it is time to face the fact that the unthinkable may just happen on your watch. Are you prepared?

❖

Dr. Albert J. Marcella Jr., is president of Business Automation Consultants, a global information technology and management consulting firm, which conducts IT audit and security assessments and provides IT audit training in diverse areas such as identity theft, privacy and cyber terrorism. Marcella's most recent book, "Business Continuity, Disaster Recovery and Incident Management Planning: A Resource for Ensuring Ongoing Enterprise Operations," is an in-depth analysis and evaluation of continuity planning procedures, methodologies and audit approaches, necessary for securing the enduring viability of 21st century organizations. For questions or comments regarding this article contact Marcella at amarcella@mind-spring.com.

■ To comment on this article, go to 1701-04 at www.drj.com/feedback.