


Top 10 Cyber Incident Pain Points: Are You Prepared?

What You Can Do To Address The Inevitable



DELTA RISK
A CHERTOFF GROUP COMPANY

A DELTA RISK WHITE PAPER | JUNE 2016



“To make no mistakes is not in the power of man;
but from their errors and mistakes the wise and
good learn wisdom for the future.”

– Plutarch



Introduction

History reveals both the good and bad when it comes to organizations dealing with cyber incidents. Among these revelations is the overwhelming fact that vulnerabilities will always be present, but it's how organizations respond to incidents when these vulnerabilities are exploited that determines their fate. Regardless of how many security controls are placed on a network and the components that go into making a network operate, there will always be vulnerabilities in a connected world. So, what do you do in an environment that allows for such risk of compromise? One of the best methods of protecting organizations is by ensuring that response capabilities are effective and efficient, and one of the most valuable steps in strengthening a response capability is learning from others'

experiences. The following whitepaper discusses the pain points that organizations grapple with when responding to incidents, and how they can address them.

Delta Risk has gathered this data from our own analysis of real world events, observations, and findings by facilitating many cyber-based exercises and conducting penetration testing in support of various commercial and federal entities. Through our interactions with these organizations, we have identified 10 trends common to most of them.

Top 10 Cyber Incident Pain Points

- 1** Lack of a cross-functional “incident commander” to coordinate response across the organization
- 2** Incident response plans lack cross-organizational considerations and buy-in
- 3** Limited data classification guidance to help determine severity and guide incident response activities
- 4** Ill-defined processes (aka “pre-thought use cases”) for responding to high impact incidents
- 5** Lack of defined checklists or step-by-step procedures, including contact lists for response
- 6** Lack of consideration of the business impact when determining courses of action for response
- 7** Ill-defined or mixed use of event and incident taxonomy between responders
- 8** Lack of defined thresholds between events and incidents to aid in decision making
- 9** Limited or lack of pre-determined (aka “pre-canned”) external communication statements
- 10** Lack of training and exercise of “memory muscle” for the most likely or high risk incidents

Top 10 Cyber Incident Pain Points

Considering the variance among industries, organization sizes, and other factors throughout the exercise data set the pain points were compiled from, it's remarkable how consistently organizations exhibited some, or all of the pain points in the Top 10 list.

1. Lack of a cross-functional “incident commander” to coordinate response across the organization

Large organizations (especially those with multiple business units or disparate functions) are often challenged by the lack of a coordination point – a “quarterback” – who is able to coordinate a response effort across multiple functions or business units within the organization. This may be due to lack of skill or simply due to lack of authority.

We find that organizations which appoint a person with visibility into business-wide impacts, and authority to make decisions across business units have been found to be more successful during incident response scenarios. Companies should also consider utilizing existing decision processes, such as crisis action teams, as a source for assessing impact.

2. Incident response plans lack cross-organizational considerations and buy-in

Incident response plans are frequently developed from within departmental silos, for example, within the organization's IT security function, and do not address the considerations of business units or cross functional areas needed to coordinate and operate together during a response. This not only leads to an uncoordinated response effort, but discourages buy-in from all business units that are expected to be involved in the response effort.

Integrated incident response plans, which account for the differences in the way business units respond, or those organizations which have standardized incident response across their functional business areas, are typically more successful during incident response scenarios.

3. Limited data classification guidance to help determine severity and guide incident response activities

Imagine that while you're reading this you were notified your network has been compromised. What data would be the priority of your concerns? Do you know where it's stored and in what formats? Does your leadership prioritize the importance of data within your network in the same manner as you? What about your HR department? Many organizations have data classification guidance, but it's typically limited to classifying data within departmental silos. This type of classification does not track where the most critical information resides in the organization, thus limiting the ability of incident responders to determine overall scope and impact of a data compromise incident.

Organizations that invest in understanding where types of information reside, and place a rating of importance on the information, are able to more rapidly make decisions, implement mitigations, and determine potential impacts when a certain type of data is compromised.

4. Ill-defined processes (aka “pre-thought use cases”) for responding to high impact incidents

Basic emergency action procedures are standard in most offices. Procedures that are followed for fire, natural disaster, and other major incidents are typically shared widely and employees are run through drills periodically so when a major incident occurs, the issue can be responded to efficiently. This level of preparation should hold the same for major cyber incidents, but unfortunately, many organizations overlook this very important component. Incident commanders are often appointed and engaged during a crisis with very limited support. It's frequently understood that incident commanders have a primary role within the organization that's sufficient to prepare them to serve in a leading role during response. However, this lack of preparation can leave incident commanders and those supporting them dependent on “in the moment” thinking; organizations stake their livelihood to their responder's ability to think comprehensively during a crisis.

Organizations should plan their response to cyber incident scenarios that may have a high impact on business operations, for example a data breach, or loss of service on a critical server. This allows the organization to respond, having thought through the considerations and major decisions that would typically need to be made during a response effort. Further, organizations should train and rehearse responders in these scenarios to increase effectiveness, speed, and consistent of response.

5. Lack of defined checklists or step-by-step procedures, including contact lists for response

Incident response is typically categorized as an IT or security function, rather than a function that should span an entire organization. Non-IT and non-security departments are often forgotten about during a cyber incident. The lack of considerations (generally, things that should be “done” or at least thought about) during an incident result in an uncoordinated response across functions.

Many responses may require input and action from multiple functions within the organization including HR, Legal, Executive Leadership, and Communications. It is necessary to plan how those various entities will coordinate and communicate with each other and with the designated incident commander. Checklists and procedures ensure incident responders are aware of the considerations and thresholds for involving other non-IT and non-security functions. Each of the functional areas like HR or legal, that support incident response, should also have its own checklist or list of considerations and contact lists as well.

6. Lack of consideration of the business impact when determining courses of action for response

The business impact of a cyber incident is something many organizations often miscalculate during an incident, much less ahead of time. Many companies are forced to wait until the incident occurs, or until a decision on a course of action is made, before understanding the extent of the impact.

Organizations that understand the impact that responses to incidents may create, are better able to make informed response decisions. Impacts may be difficult to predict for all but the most high-risk or well-thought scenarios, but organizations which have ready access to staff who understand how to determine potential impacts for a given incident, can more effectively chart a course of action to minimize impacts.

7. Ill-defined or mixed use of event and incident terminology between responders

Just as there are differences of taxonomy when it comes to physical incidents (tornado watch v. tornado warning) there are differences in taxonomy when it comes to cyber incidents. Common event and incident terms that are often confused include “alert,” “event,” and “incident.” Some organizations mix terms during an incident response effort, causing confusion among responders and decision makers.

Organizations that standardize, publish, and consistently use the same taxonomy are more effective at responding as intent and meaning are immediately clear. The actual terms used are mostly irrelevant, provided everyone is using the same taxonomy. When non-standard terms are used, organizations face challenges when coordinating with external entities.

8. Lack of defined thresholds between events and incidents to aid in decision making

Triggers and thresholds help organizations determine when to take action. Lack of clarification on when an event escalates into an incident and lack of thresholds for determining when to trigger certain response actions is a commonly missing component. This introduces challenges when determining when to communicate with senior management or involving law enforcement. For the most part, organizations realize after the fact that their thresholds aren't well-defined, and many senior executives stated they would want

to be involved earlier in the response, even if it was just from an informational standpoint.

Rigorously defined thresholds for key use cases or high impact scenarios, and understanding when to escalate activity, allow organizations to rapidly make decisions and not get stuck in “analysis paralysis” with regard to what actions to take and when. These thresholds can also remove the “should we?” debates that often occur during incident response and allow responders to focus on action.

9. Limited or lack of pre-determined (aka “pre-canned”) external communication statements

Internal and external communication is critical during incident response and most organizations have some type of communication plan which addresses when to communicate and how to tune the general tenor of the communication. However, most organizations stop there and fail to create holding statements or other pre-defined communication templates, resulting in missed or delayed communication opportunities, or worse, wrong information being released from multiple points. In certain instances, communication statements were not coordinated with the IT security functions, resulting in a business operations focused message that did not convey “security’s message” effectively.

Organizations that have a clear media and communication policy, coordinated by a central function that addresses operational, security, and management perspective through use of a template, have a good handle on crisis communications during a cyber incident.

10. Lack of training and exercise of “memory muscle” for the most likely or high-risk incidents

The notion of “practice makes perfect” applies in many situations, and holds true for cyber as well. Many organizations are good at handling events like fire or evacuation drills, having had repeated opportunities to refine the response process and train staff on

how to handle these events. However, many organizations do not practice for cyber events, or more specifically, their highest risk or most likely cyber scenarios. This results in organizations reacting to a major incident for the “first time,” as it occurs. In these situations, organizations get little benefit from past experience and lessons learned, and frequently struggle to fight through the incident, figuring it out as they go.

Through exercising and training to the most likely or riskiest scenarios, organizations build muscle memory, and are able to respond in a manner that benefits from having thought through the response. Simply put, organizations which capture the processes used and lessons learned during an incident, and then apply and practice them in periodic exercises are better prepared and can respond more effectively in a coordinated effort.



Additional Pain Points

There are a number of pain points that can affect an organization's incident response capability, therefore this list shouldn't be considered comprehensive. Rather, the additional pain points below should be "considerations" for examining your organization's response to cyber incidents.

Limited capability and visibility into Data Loss Prevention (DLP) and network traffic monitoring

Many organizations have Data Loss Prevention (DLP) capabilities, however, most organizations are unprepared on using DLP as an integrated part of responding to an incident. Further, many organizations have limited visibility into DLP alerts, many times relying on weekly reports to identify activity. DLP can provide an effective method for identifying compromised points in the organization, as well as help identify the scope of an incident. Responders should consider DLP as a data source for triaging an incident, and they should have near real-time access to alerts, the ability to create custom signatures for detection, and to generate reports on an as-needed priority basis to help with response. Related to DLP, organizations often place precedence on perimeter defense and detection, and neglect threshold detection methods within the network regarding traffic especially regarding drops in network traffic. Increases in network traffic are often considered as denial of service attacks and appropriately handled. However, decreases in network traffic usually don't receive the same treatment from a response perspective even though sudden decreases can be indicative of issues in much the same manner as sudden increases in traffic. Both DLP and network traffic monitoring should be considered not only as detection, but also as triage tools.



No connection between HR/Physical Security/Compliance and IT Security

Consider the case that HR has just terminated someone's employment with your organization due to theft of company property. Was the account disabled immediately, what information did the employee attempt to steal? Did HR personnel notify the IT and security staff to simply disable the account, as is traditionally done, or did they provide enough detail such that IT security could open an investigation to determine the extent of the theft? The lack of communication is a dangerous void in cyber security, especially in the case of incident response. Consistent information sharing among these functions can help identify incidents and add context to help triage incidents.

Over-reliance on Law Enforcement

Law enforcement agencies can assist with investigating data breaches or intrusions. However, organizations should not consider law enforcement as a substitute for their own triage, analysis, and response functions. Law enforcement is an external agency; they may not be able to respond to your incident on timelines you need, nor in a manner consistent with how you need the incident to be handled. Law enforcement has different goals, priorities, and stakeholders than you do. While law enforcement is excellent follow-up for purposes of prosecution and information-sharing, it can at times create a handicap for organizations. Law enforcement relies on you to monitor your own networks and appropriately track your actions during incident response in order to even begin to prosecute or conduct any basic investigation. Law enforcement can make for an effective partner in response, however, they should not be viewed as a panacea for handling incidents.

Lack of single sign-on access management

Access management is a frequent recurring pain point for organizations, especially when incidents which take advantage of single sign-on or centralized access schemes occur. Single sign-on is popular with many organizations because of its simplified management. However, it's the security implications of a compromise within single sign-on that organizations lack understanding of. When critical systems are integrated with single sign-on, we have seen two issues arise. First, a compromise of single sign-on results in a much broader compromise of the critical systems, which may not be considered by incident responders. Second, as responders start to curtail access by disabling accounts in single sign-on, users may not be able to get into critical systems that may otherwise be unaffected. Single sign-on presents unique challenges and potential for impact that responders and their documented plans should consider.

Limited understanding and guidance on role and authority of incident commander

One of our top 10 pain points identified the need for an incident commander. In addition to designating someone as an incident commander, there must also be roles and responsibilities identified for that position, as well as a solid understanding of that position's authority to make decisions in response to an incident. It's frequently in the authority area that organizations struggle with the incident commander role. For example, can the incident commander order a shutdown of a critical e-commerce server that will clearly cause a business impact, if it was determined to be a course of action during an incident? Defining the expectations and authorities of this position allows the incident commander to make decisions based on established guidance, significantly speeding up the response effort.

Response team and management construct activation thresholds are undefined

It's not always clearly identified in an incident response plan at what point during a possible event should the computer incident response team (CIRT) or other management constructs (e.g. an enterprise-wide crisis action team) be activated. Organizations will typically have an enterprise-wide crisis action function tied to a physical disaster. These constructs may be used for cyber response as well, but at what point does the incident go beyond just the incident commander? The thresholds and criteria for activating and involving these constructs should be identified to help the incident commander determine courses of action.

Lack of incident classification or categorization

Did the incident result in a public data breach, or simply a corruption of files with no exfiltration of actual data? While both of these are harmful to an organization, one may be more harmful than the other, and each has its own response requirements. A proper categorization of incidents (for example, critical, severe, medium, low when categorized according to impact) allows incident response to shape the response appropriately, not over or under reacting.

Lack of communication protocol among incident response entities

Organizations should determine the methods in which all stakeholders involved in a response effort will communicate. With large groups, a single teleconference can become unwieldy and ineffective. Individual teleconferences may result in information being missed by groups that do not participate in those calls. Further, the medium by which these communications are made (e.g., VoIP, internal phone bridge, email, cell phone), may be affected or compromised based on the incident. A balance between communication methods, mediums, and tracking information (see next point) related to incident response, is needed.

Lack of centralized incident management information tracking and reporting

A centralized incident tracking capability is often an afterthought, with a significant incident usually triggering the revelation that a solution is needed. When gathering information and dispersing action items to many individuals throughout multiple functional areas there must be a central repository for to-do's, actions taken, and milestones along the way. This not only assists with maintaining sanity during an incident response, but also allows organizations to look back post-response and evaluate in an effort to improve their efforts. A solid information management system can also help with communicating status updates (see next point) and in keeping a dispersed team informed (see previous point) with established communication protocols.

Lack of defined status schedule update for high level incidents

Status updates can paralyze a response activity. An incident commander will be useless if they are calling functional areas for status updates and funneling updates to management throughout an incident. A pre-determined status update schedule, that's aligned with incident categorizations and management expectations, allows the incident commander to prosecute the incident while keeping appropriate parties informed on a set schedule. The use of an incident information management system (see previous point), can be used in conjunction with a status update schedule to allow management and other stakeholders to obtain the latest status information, allowing the incident manager to focus on response.



No succession plan in place for Risk & Incident Management roles

Organizations often believe that designating someone as incident commander is good enough. It isn't. A single point of knowledge for something like incident response is a single point of failure. Often, organizations appoint their most knowledgeable individual as an incident commander, but do not appoint an alternate. Invariably, incidents occur at the most inconvenient time, and organizations should strive for continuity, not only within the role of incident commander, but also for security roles within individual business units. Each functional area should have both a primary and alternative to handle for cyber incident response procedures in the event that one isn't available due to rudimentary reasons like travel or unforeseen circumstances.

Culture of siloed operations and response

One of the most debilitating items that can affect an incident response capability is a culture of functional areas isolating themselves, their information, and their actions from everyone else in the organization. At times this can be the result of a functional area not wanting leadership to find out about an incident, but it can also be due to a mindset of "we'll handle it at the lowest level". Regardless of the reasoning, this insularity can be a dangerous trait within an organization. The sharing of information (including bad news) within an organization should be encouraged so that an issue such as a possible intrusion can be addressed immediately.

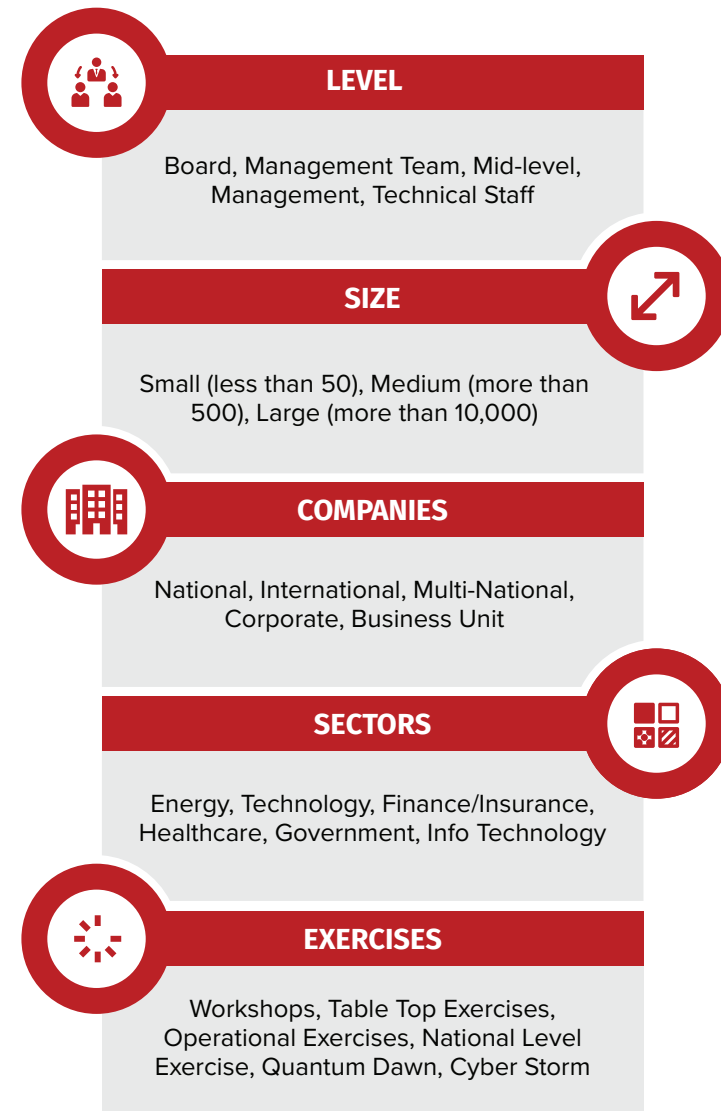
Where did these pain points originate?

The pain points were derived from a series of cyber exercises conducted by Delta Risk over the past seven years. The exercises were discussion-based (table top) and operational in nature, and involved companies of varying sizes from different sectors including healthcare, technology, financial services, government, and manufacturing. Organizations were presented with a cyber scenario and asked to respond in a manner consistent with their current capabilities and processes. The common pain points stem from our own observations during these exercises and represent issues that affect most companies when presented with a cyber incident. Cyber exercises are used to determine how an organization would respond to a given cyber crisis. Exercises can provide a wide spectrum of opportunities for organizations to identify procedural gaps, organizational shortfalls, and even technical vulnerabilities as they react to a given situation.

Table top exercises provide an informal, low-risk method of accomplishing this, while operational exercises provide a stimulus and opportunity to observe a realistic response. During an exercise, participants are presented with a hypothetical situation, and must discuss how they would respond. In the case of table top exercises, participants are asked to demonstrate decision making (who is making the tough decisions), coordination (who is talking to who), and actions they would take if the scenario were to occur. Table top exercises are discussion-based, meaning participants only discuss actions they would take – they do not actually perform the actions – resulting in zero impact to ongoing operations. Participants are welcome to refer to guidance or documentation as needed during the exercises – they may go so far as to call other people to discuss ideas or solutions – but the exercise is limited to discussion only to minimize risk to operations and maximize opportunities for learning and observation.

Pain Points

Deriving Common “Pain Points” to Cyber Incidents



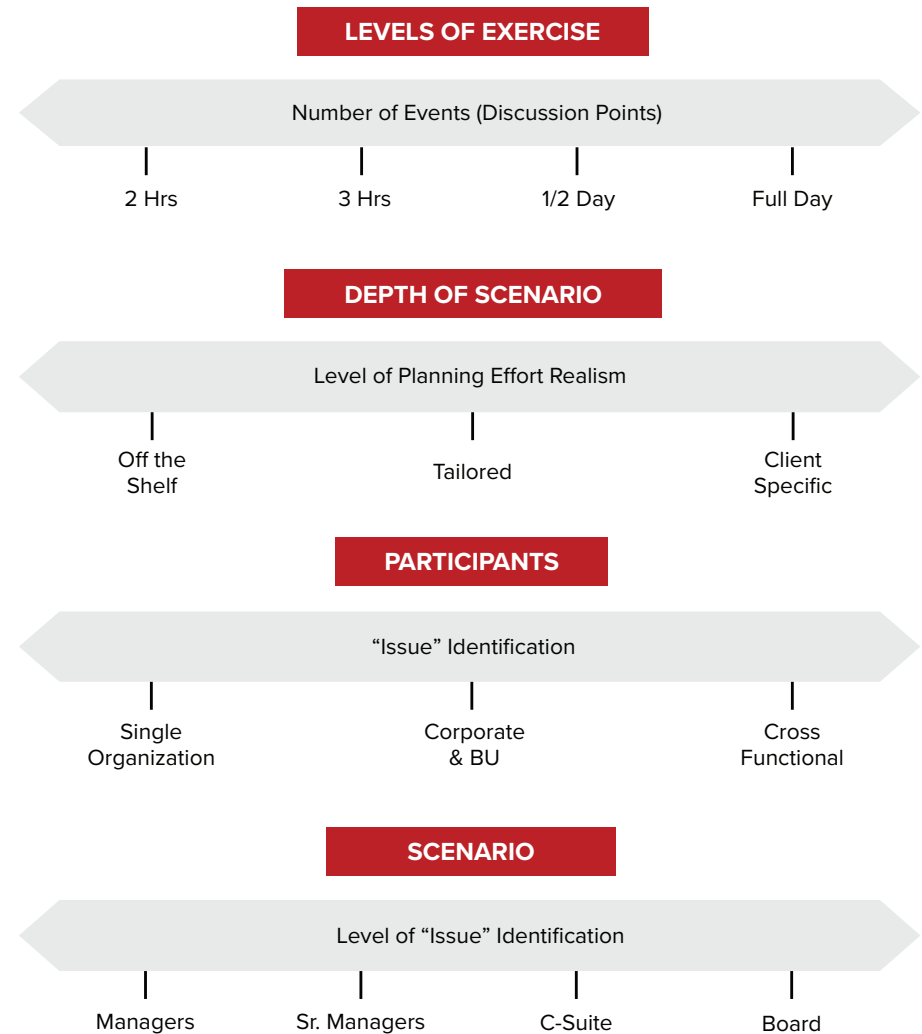
Generally, there are four levers which can be adjusted to customize a table top exercise for an organization:

- 1) Length – the length of time allocated for the exercise; ranges from one hour to multi-day.
- 2) Depth – the level of realism in the presented scenario; ranges from “off-the-shelf” pre-canned exercise to fully customized exercise scenario tailored to the organization specific risk concerns.
- 3) Participants – the organizations involved in the exercises; ranges from single organization to cross-functional participation from multiple business units.
- 4) Level – the level of the participants; ranges from technical staff to C-Suite executives from multiple business units.

Operational exercises focus on the key processes, procedures, and capabilities stakeholders and responders use during a cyber incident. Operational exercises put the participants into motion and ask them to take action as if the scenario presented were actually occurring. These type of exercises help to discover gaps in processes and instill “muscle memory” by allowing participants to practice the steps they would take during a response effort. Operational exercises present a hypothetical situation, and much like table top exercises, Length, Depth, Participants, and Level are adjustable levers for planning the exercise. An ideal operational exercise is run with participants at their desks or place of work. This increases the accuracy of response times and permits the possibility of real world distractions or technical issues; the realism allows the observation of the “devil in the details” and gives organizations much more fidelity in the results.

Table Top Exercise Design Options

Four Independent Principles



If needed, a hybrid exercise, consisting of both a table top exercise and an operational exercise can be used. This allows, for example, senior leadership to participate in a short duration table top discussion, while the security staff participates in an operational exercise. The two can be run sequentially with the results from one exercise feeding into and affecting the scenario for the other. This ability to mix and match different exercise types, scenarios, and participants allows organizations to drive to the precise effect or outcome they want.

Conclusion

When considering the strength of an organization's cyber response capability, a strong focus on preparation is key. The steps to proper preparation can be developed from the failures and successes of other organizations. With the backing of a wealth of experience from conducting exercises throughout a wide variety of industries and organization sizes, the list of pain points provided gives insight into voids that may be present within your organization's current cyber response capability. These and more pain points can be revealed through a solid cyber security training and discovery program that involves a consistent and thorough exercise component.



About Delta Risk

Delta Risk LLC is a global provider of strategic advice, cyber security, and risk management services to commercial and government clients. We believe that an organization's approach to cyber security should be planned, managed, and executed within a tailored and organization-specific program. We help guide organizations to succeed in today's cyber environment by building on the people, processes, and technology they already have.

<http://www.delta-risk.net/>
info@delta-risk.net

106 S. St. Mary's St., Suite 601
San Antonio, TX 78205
(210) 293-0707

4600 N. Fairfax Dr., Suite 906
Arlington, VA 22203
(571) 483-0504

