MIR3®
INTELLIGENT NOTIFICATION
An ECN Company

How to Develop an Effective Cyber-Response Program

By Cheryl Carmel
CISSP, security officer for MIR3, member of ISC2

Table of Contents

Every day we hear about cyber attacks, from those impacting large retailers to small businesses, hospital systems and even esteemed financial institutions—virtually any organization is at risk. And as these hackers have succeeded in slipping through the defenses of people and organizations as diverse as the Pope and the Pentagon, they're probably capable of infiltrating your organization too.

Close on the tail of these alerts is often the revelation that proper security had never really been put into place, or was put in too late. Perhaps worse is the realization that the breach may be weeks or months old, and that cyber criminals have been stealing data all along. Fingers are pointed, a brand is tarnished, customers and clients are frustrated, and someone in the highest ranks is likely to lose their job or even go to jail.

What if something like this happened to your organization? Would your cyber insurance cover the liability? If you have a cyber-response plan in place, is it sufficiently broad in scope? Is there a training program in place and are the right people engaged in it?

In this brief we'll share what you need to know to properly assess your plan, persuade your executive management team to provide you with resources, and build a program that will help you prepare, prevent and practice a comprehensive cyber-response plan.

Build the program

Any size of business, in any industry, must have a cybersecurity program that includes a cyber-response component. Let's explore the steps needed to build your program, followed by the steps of implementing the program.

Ultimately, you want your program to prevent cyber issues in the first place. But you also have to be prepared for issues when they arise, and you have to practice and exercise your plan in order to be prepared.

PREVENT

The preventative stage is the build-out of the entire cybersecurity program. There are many excellent standards you may follow for this, including ISO 27000 and the NIST series. As prevention is a vast topic, we'll cover it more specifically in a future webinar and paper.

PREPARE

Secure executive sponsorship

To build any program, you need support from the highest levels of the organization. If you've already secured support for your cybersecurity program, support for the cyber-response program should be a given. However, don't assume that your executive team knows how critical this part of the program is. Executives often state that preventing damage to the company's reputation and brand is paramount—use that insight to explain and show that cyber incidents come with both hard and soft costs, many of which are virtually impossible to recover.

Data breaches don't only hurt your business, but harm customers and, potentially, their customers and consumers as well. Breaches often involve investigations from law enforcement and government, and can spur audits by industry bodies and even by your larger customers. And, of course, breaches often invite lawsuits.

The Ponemon Institute states the average cost of a data breach in the U.S. was over $7.7 million in 2015[1], which means about $215 per record lost. By making your executives aware of numbers like that, you can often gain the support you need for a solid information-security program.

Understand your scope and assets

The next step is to define the scope of your program and understand your inventory of assets. Many scope statements emphasize customer-facing systems. This is a great first step, but it's critical that internal resources are engaged as well.

Hopefully, your information security and business continuity programs have already completed an asset inventory of people, process, technology and data. If not, this is a good time to do so. If your inventory is already completed, now is a good time to review. Use this review to focus on scope and assets mentioned above as they relate to cybersecurity incident response.

To help ensure complete coverage of assets, start by taking a lifecycle view of your business processes by thinking through the beginning, the middle and end of each process. For example, a human-resources lifecycle business process includes recruiting, hiring, training, performance reviews, job transfers, promotions, and ultimately, termination of employees. Each step will include assets in each category.

In the people asset category, be sure to include not only internal resources, but also third-party resources such as part-time and temporary workers as well as contractors.

Business processes occur throughout the organization; there will be obvious processes to review, and then subtle ones that may not have previously been considered. Most business process will have some policy or procedural documentation to support it—don't forget to include this in your inventory.

Another example is the system development lifecycle for your hardware and software. This can be vast; inventories must include details from operating systems to versions and service-pack levels. The same should be documented for any database management systems, Web services and applications that manage hardware. Be sure to include all services running on systems, open and explicitly closed ports, wireless systems, phone and fax systems, security cameras, door-access systems, and point-of-sale systems. Be sure to include all mobile apps on all devices, like the point-of-sale device that may also be your phone. Don't forget the huge amount of open-source software that is part of modern business.

Each and every one of the above has data, and you want awareness of each data element associated with each of these areas. Remember: data is the primary target for cyber criminals—you need to know what you have and where it lives to protect it.

> Remember: data is the primary target for cyber criminals—you need to know what you have and where it lives to protect it.

Identify the risks for each area

With this information in mind, what risks do you need to consider based upon your business? Who would want your data and why?

What is the probability of a threat agent (a person, a hacker) successfully deploying a threat vector (virus or malware) to exploit a vulnerability (security bug, software weakness) that has weak or no preventative countermeasures (firewall, patching) and the associated impact (incident or breach) that event will cause?

As you think through the risk statement, include each of these risk areas that need review:

- Natural or human risk, which can be either accidental or malicious
- Physical risk, which can include lost or stolen devices, as well as broken locks
- Technology risk, which includes all hardware and software
- Data risk, by individual element, in every location the data resides and by each technical or human access method

Collecting this threat intelligence is crucial as each data element provides cyber criminals fodder for funds or misuse. Cyber criminals are after whatever data they can steal to sell, to hold for ransom or to use as a weapon.

Just as each element of data has its own set of risks, each has a value. Simple personal data such as name, email address or phone number are all valuable. If the data spans nations, it has more value. Add health information, Social Security numbers, any financial data and the bounty goes up even move. Top that off with background-check data, military records and special categories of data such as religion, sexual orientation and political affiliation, and the value of the data increases exponentially.

When a cyber criminal gathers data that people have volunteered...and combines that with stolen data, they are then able to paint a picture that can be very useful in making money and wreaking havoc.

When a cyber criminal gathers data that people have volunteered, such as that easily collected from social media sites, and combines that with stolen data, they are then able to paint a picture that can be very useful in making money and wreaking havoc. Each location that data is stored increases that risk.

Your infrastructure and all your applications have vulnerabilities too—no hardware or software is without flaws. Knowing the threats, vulnerabilities and control weaknesses should make you wary of storing information in multiple locations, as each adds to the threat landscape.

Another risk is posed by access; each person that has access to your data increases the risk. Unfortunately, humans are often the weakest link in the cybersecurity chain. According to the *Proficio Survey of Cybersecurity Challenges*[2], the number-one worry for IT security professionals is that of insider threats, whether deliberate (from disgruntled or former employees) or accidental (careless staff or contractors).

Knowing that threat agents include your employees, and data accessed through employees is susceptible to virus and malware infections through simple spam and phishing attacks, should make the principle of least privilege easy to enforce.

Identify framework and controls

Fortunately, depending on the industry your organization belongs to and the type of data you need to protect, your framework could already be set by outside standards. For instance, if you accept credit cards you must comply with PCI. If yours is a financial institution, FFIEC is your ruling standard. If your organization handles medical information, HIPAA will provide a set of standards and oversight.

If you don't already follow a regulatory standard, choose a general security framework like one of the following:

- ISO – Well-known international set of standards
- NIST – Established US set of standards that are required by federal government agencies
- AICPA – Familiar auditing standards for service organizations
- CSA – Fairly new and upcoming standard directed to cloud service organizations

Understanding regulations related to privacy of information is a special area, and a critical one, as there are a multitude of privacy laws around the world. All but three of the United States (Alabama, New Mexico and South Dakota) currently have unique privacy laws. Other localities, such as Washington D.C., Guam, Puerto Rico and U.S. Virgin Islands, each have their own laws.

If your organization handles international data you need to be aware of General Data Protection Regulation (GDPR), which replaced the EU Data Privacy Directive, as well as the regulations of each international country, as each has its own version. And of course we now have Privacy Shield, which replaces the Safe Harbor provision. All of these different

standards, regulations and provisions mean that if you have a breach of personal data, you will most likely need an attorney who specializes in privacy law.

Some breach laws state that notification of individuals that have been breached must be sent as soon as unauthorized access to data is suspected. Other laws are contradictory and state you must wait until you are certain the unauthorized access has occurred. One law states that you must fully inform the individuals how the incident occurred; another states you must not provide any information regarding the nature of the incident. Again, it's wise to have an attorney who specializes in such matters close at hand.

Identify the cyber-incident response team

The establishment of a cyber incident response team is a critical step towards managing any cyber incident. The cyber-incident response team (CIRT) is comprised of the technical resources required to detect, diagnose and isolate a cybersecurity incident. Your team members must be identified prior to an event, but as each event is unique, so is the actual team you pull together at time of the incident. Note that your CIRT is different than your incident management team (IMT), though they do work together.

Members of your CIRT will include:

- **Team lead** – The lead will keep a focus on minimizing damage and recovering systems quickly, while also guarding the team from interference so they can do their jobs. The team lead is on point until the situation is resolved and operations are back to normal. They may coordinate some functions with the business continuity crisis response team as well.
- **Investigators** – Think of this team as your detectives, a technical team made up of specialized and talented internal individuals (and possibly external individuals). Your lead investigator, or technical resource, will determine the actions the rest of the team will perform and process feedback from the rest of your resources.
- **Forensics expert** – If you're fortunate, you'll have a skilled person on staff to drive diagnosis and isolation. If not, you must have an IT person that is sophisticated enough know when to call a forensic team in.
- **Communications** – Many regulations and customer contracts have strict requirements for information sharing. This communications person will document the minute-by-minute actions of your team, tracking the details of the event as it unfolds. They will also manage the flow of information going the other direction, towards the rest of your CIRT. All this information may also be used for legal discussions, media presentations and to keep executives informed.
- **Customer-facing individuals** – These people will communicate with internal as well as external stakeholders and could be made up of helpdesk personnel, customer support or account managers. They must be trained to provide only the information they have been instructed to provide, and only when instructed to provide the information.

The incident management team

The IMT has the CIRT team leader as a member and will also include legal, human resources, marketing, appropriate business-line owners and executive management. You only want executive management as part of the incident-response team if they have the technical skills to do one of the jobs needed.

The cyber-incident response program

Your organization probably has a policy management structure to follow. The framework provided here includes high-level policy requirements followed by a series of more detailed procedures, plans, playbooks, templates and checklists. As with any documentation,

write what you need—not too much and not too little. If you have specific industry requirements, follow them. If your organization does not have specific legal or industry regulation requirements, but you support business customers that do, you need to be aware of those requirements as well.

Here's a simple outline to define and build policy, procedures and plans:

- Incident management policy
- Procedures for reporting
  - Reporting templates
- Plans for communications
  - Communication script templates
- Playbook for event handling
  - Checklists for specific events; knowing you can't plan for all events, choose which are more likely.

PRACTICE

After all the preparing, it's now time to practice. Practice will increase familiarity with your plan and will help create a culture of awareness throughout the organization.

Awareness

Training is integral to a culture of awareness, so develop a training program that is informative and engaging. This can be done as a part of the information security awareness training or business continuity training—as long as there is sufficient emphasis on the cyber-incident aspect. Consider training all employees specifically on the subject of cyber awareness so they understand their roles in the event of an incident.

Exercise sessions could be a series of tabletops that would eventually include all employees. For a helpdesk or customer support team, describe a series of events and ask, "If this action were to be noticed, would it need to be reported? What would you do next?" Use similar exercises for the sales and marketing teams.

For the IT team, perform a series of incident-based exercises from ransomware to high-volume traffic on a specific port on a firewall and ask what action steps would be followed—by whom, and when. Follow up with real-life scenarios using an independent consulting firm or a simulator environment. Invite your executives to participate in a spear phishing exercise along with a member of the incident management team to practice full response.

Practice will increase familiarity with your plan and will help create a culture of awareness throughout the organization.

Operationalize the plan

When it comes down to it, machines can only do so much. The human, thinking and aware side of the business is what really matters in times of threat. Tools automate a lot of the process but they will never be able to do it all. For example, say you have a person who struggles with passwords. Their behavior may send up a flag that an interloper is trying to gain entrance, but human intelligence reminds us that for that individual, this behavior is normal.

Take full advantage of your human intelligence and operationalize your plan across all business groups rather than keeping it in silos. Your plan must be incorporated into the day-to-day operations of every employee, especially your technical teams. All employees should be required to annually review the plan and be familiar with security topics such as event identification and reporting. Remember:

- Your plan needs to be part of everything, and all employees need to be part of it
- Add goals and objectives to performance reviews for accountability
- Incorporate CIRT plans into your standard operating procedures (SOPs)
- Review system monitoring requirements regularly to look for new threats and anomalies

Continuous review and improvement

As with any management program, follow the Deming's Cycle of PDCA (plan-do-check-act) or a similar protocol. It's a good idea to create a committee that can review the security posture, specifically the incidents that have occurred, with the executive team.

Your security committee should also hold regular reviews of policy documents. Note that specific attention to policy documentation must also be done after an event has occurred to allow for updates to policy in a timely fashion.

The cyber-incident response team will work with the incident management team to create a report after each incident. The report will describe the incident, the corrective actions taken, and any new controls implemented to prevent future incidents from taking place.

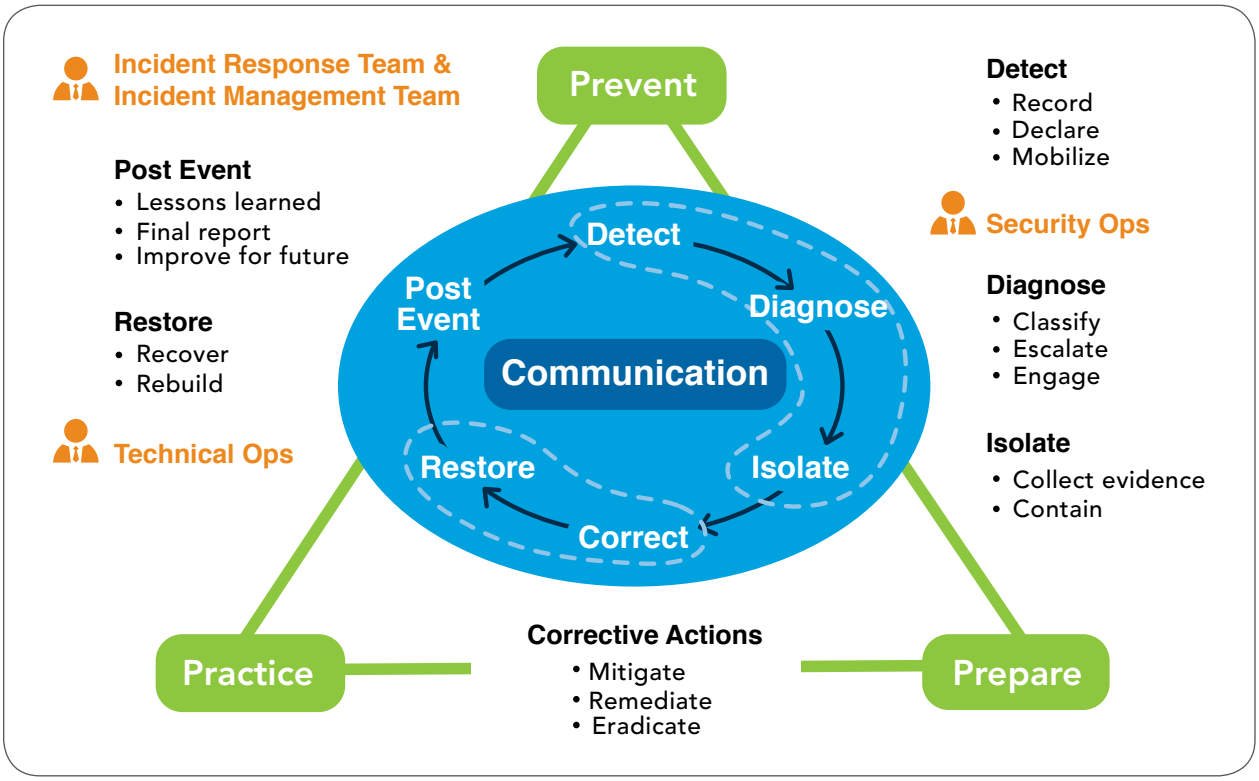
PERFORM

Follow the program

You've completed your prevention measures by implementing an information security program, you've done the preparation work by creating the cyber-response program, and you've applied practice exercises to be ready. The call comes in and a breach has occurred … what do you do?

It is now time to perform!

The response to any kind of cyber incident is a business process, a collection of procedures aimed at identifying, investigating and responding to potential security incidents in a way that minimizes impact and supports rapid recovery.



A graphical representation of the incident-response program.

Detect

The security operation team moves into action as soon as an event is identified.

Record

A security event is a single instance that may pose a negative impact on your information environment. When any event is detected, it must always be recorded. Events do not always lead to incidents, and incidents do not always lead to breaches, but all breaches start with an event.

> Events do not always lead to incidents, and incidents do not always lead to breaches, but all breaches start with an event.

All employees have some level of security awareness based on their position in the company. Your staff often knows when something is just not right, and this insight is key to detecting events. Customer support may suspect something from listening to customers, help-desk will notice anomalies by paying attention to internal inquiries, your operations team is constantly reviewing and monitoring infrastructure—all of this provides a tremendous amount of intelligence.

Use this intelligence; report who saw what, and when. If all reports go to a centralized system that employees have access to, this can trigger action with your CIRT. The type of event will determine who is needed to take action and what action to take; this could range from a quick review to a longer investigation, even one that could take months to complete.

Declare

A security incident is a major event or collection of smaller events that has led, or will likely lead, to a significant negative impact on your business. All events, even small ones, should be reported and reviewed. You can then determine if an investigation is needed. Your team will look for a possible common denominator and try to think like an attacker. Attackers are in general lazy and looking for the easy target, but they are also persistent in looking for a generous target.

The team may reach out to your ISP or CSP to see if they've detected any suspicious traffic. The attacker's methodology starts with reconnaissance; they'll scan for open ports and system or application vulnerabilities to take advantage of, and these efforts leave tracks.

Once an attacker penetrates the system and starts to move around, they can be nimble, pivoting from one environment to another. They then deliver their payload, installing evil software to exploit and gain command and control of your system.

Undetected, they can actively capture information over time. The assault will continue until they get everything they want. Then they leave, but not before weaponizing, ransoming and terrorizing your system. Remember: Time-to-compromise is measured in minutes; time-to-discovery is measured in days, months and years.

As you prepare to mobilize, ask if your team has the skills to manage the event; do you need to engage outside help from a forensics team?

Mobilize

Now your CIRT will meet and begin internal communication with the IMT. At this point, it's very important to know the depth of knowledge and range of skills of your internal staff. Do not hesitate to reach out to external resources you may need to work through the incident. This is when executive management needs to offer support by procuring additional resources, while staying out of the way of the technical team so that they can focus on the incident at hand.

Diagnose

Classify

As part of the report, the incident will need to be classified. Classification will align with your framework of standards. Incidents fall into three broad categories:

- Physical – such as
  - Dumpster diving
  - Theft of device

- Human – such as
  - Social engineering
  - Malicious or unintentional insider
- Electronic – such as
  - Denial of service (DoS)
  - Malware, botnets and virus, Trojan, worm

Use the incident classifications that are available for your industry or classify items specific to your business.

Escalate

As you learn more, you may need to escalate your actions, always in close communication with your IMT. If you determine you have an actual breach (unauthorized access or acquisition of a system or data), it's time to escalate to outside counsel and a breach remediation specialist.

> Remember: Time-to-compromise is measured in minutes; time-to-discovery is measured in days, months and years.

Isolate

Contain

Once the threat has been properly diagnosed you can be more certain that the threat is contained to specific components. The outcome of the diagnosis phase allows you to start evidence collection.

Collect evidence

Your team or outside experts must be qualified to collect evidence that could be used during any formal governmental investigation. Do you have a Legal Hold Notice on any activity or data? Are there other legal requirements you need to be aware of? This is particularly important if sensitive data is part of the attack or if international individuals are included in the victim list.

Corrective actions

Now your technical operations team will get involved. Depending on the severity of the damage, technical operations may be able to fix the systems, or if the damage is severe they may need to build new systems.

Mitigation will lessen or reduce the possibility of further damage. This first step may be accomplished by installing a temporary patch or implementing a quick additional control, ensuring up-to-date patching has been done on all components.

A more permanent corrective action, remediation, may be accomplished by removing an old hardware or software component that can no longer be patched, installing another vulnerability-management layer and implementing strict, permanent controls to prevent the vulnerability from reappearing.

In those cases where the system is very badly damaged, the only option may be to completely wipe the system or physically destroy it to eradicate the issue.

Restore

The last phase for technical operations is to return the system to normal operation. They will implement whatever actions are needed to recover your data and rebuild any damaged systems.

Post-event activities

Now the CIRT and IMT should meet as soon as possible while all the information is fresh in mind to document all steps taken. The final report could be an internal report only, or it could be used, if necessary, for legal action. Ensure the report is factual and stick to the technical details, leaving out criticism and commentary. Double-check that the report is accurate and the timelines match. The report should be reviewed and approved by the leader of the CIRT and the IMT.

Take the time as well to review the preventative controls that are in place as well as the performance of the CIRT and make appropriate improvements to the security and response programs.

Communication lifecycle

Communication is key to managing any kind of crisis, and a cyber event is no exception. As in so many business cases, an automated emergency mass notification system (EMNS) can ensure that the right message is communicated to the right people at the right time. A notification system is not an afterthought, but an integral piece of any comprehensive cybersecurity program.

As we worked through this event, communication was occurring throughout, both internally and externally. Note that notification of every person touched by a cyber event is often legally mandated and can very specific. Be sure to use a system that allows you to fulfill your legal communication obligations and track and report all messages and responses.

As mentioned during the performance stage, communication to outside counsel, forensics and other security expertise as well as law enforcement is fully integrated. After the event some industry agencies or regulatory bodies as well as the cyber-insurance agency may require copies of the post-incident report. Communications may include information-sharing groups as well as specific groups established by the Presidential Decision Directive 63 (PDD-63) in 1998.

Summary

Start by gaining executive support for your program by presenting information that is relevant to business goals. Collaborate with all business units to collect common information, and make use of one, or many, of the standard methodologies that have already been tested and are known to be effective.

Know your world; know the strengths and weaknesses of your program and your team, and know when to supplement externally. Make the program part of daily life; the more comfortable your team is, the better they perform at time of need.

Bonus Material:
Forensic Support Checklist
on next page

This paper is based on the webinar, *How to Develop an Effective Cyber-Response Program*, presented by Ann Pickren, BC/DR expert, MBCI, and president of MIR3 and Cheryl Carmel, a member of ISC2 and security officer for MIR3.

For more briefs and other helpful resources, visit: www.mir3.com/resources

---

[1] 2015 Cost of Data Breach Study: United States, by Ponemon Institute
http://www.jmco.com/media/Ponemon-Data-Beach-2015-Report.pdf

[2] Proficio Survey of Cyber Security Challenges 2016
http://www2.proficio.com/l/16302/2015-01-07/hmbr5/16302/79424/Proficio_IT_Security_Survey.pdf.pdf

MIR3: Proven technology, global reach

MIR3, an ECN company, is the leading developer of Intelligent Notification and response software, which helps companies and organizations enhance communication abilities, protect assets and increase operational efficiency. MIR3 technology enables advanced, rapid, two-way mass communication for IT, business continuity and enterprise operations.

Forensic Support Checklist

Your forensic team will achieve success sooner if you provide the resources they'll need soon after an event has been discovered. Use this checklist to prepare:

Infrastructure diagrams complete with:

- ☐ System names with the primary purpose
- ☐ System administrator and owner
- ☐ Details of each system's operating system version and patch level
- ☐ Details of each system's application and services running
- ☐ Firewall rules with explicit open ports
- ☐ Configuration file information
- ☐ Interconnectivity between systems

Data flow diagrams with:

- ☐ Details of data elements in each database or file
- ☐ Data administrator and owners
- ☐ Details of where the data flows from and to
- ☐ Data retention policy by data element
- ☐ Locations where the data is stored, by server, backup (tape, vault and other means)
- ☐ Access methods by human user and application or system user

Audit files including:

- ☐ System and network audit files
- ☐ Security audit files
- ☐ Application audit files
- ☐ Access control including physical access to doors and cameras

NOTE: Review your organization's audits regularly to ensure auditing is turned on and collecting appropriate data. Ensure the audit files are collected in a centralized and secure log collection system.

External contact resources:

- ☐ Forensic expertise, security consulting firms
- ☐ Breach remediation
- ☐ Cyber insurance
- ☐ Law enforcement, local police, FBI, states' attorneys general
- ☐ Regulatory bodies from the industry, domestic government, international government
- ☐ Outside legal counsel
- ☐ Information sharing centers
- ☐ Internal resources including staff, tools and toolkits, policy, and documented information.

The first step is to disconnect the system or systems from the network by unplugging the network cable or disabling the wireless card—but leave the power on to retain critical data in RAM. Note that the cybercriminal may have installed a utility to turn wireless back on, making your efforts to disconnect from the network invalid, or even to alert them to trigger retaliation. **This is why connecting to the right forensic technical experts is paramount early in your investigation.**