CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Computer Forensics for Business Leaders: A Primer

Key Message: Computer forensics is often overlooked when planning an incident response strategy; however, it is a critical part of incident response, and business leaders need to understand how to tackle it.

Executive Summary

Computer forensics may seem daunting to business leaders, because it evokes images of specialized equipment and knowledge. However, the most important part of computer forensics is creating a solid response plan and knowing when to involve outside experts. All businesses can achieve this level of computer forensics readiness.

In this podcast, Richard Nolan, who leads CERT's computer forensics efforts, shares what business leaders need to know and provides pointers to resources that can increase organizational preparedness.

PART 1: FRAMING THE ISSUE

Our governing perspective for this podcast is: What do business leaders really need to know about computer forensics?

First, some quick definitions: Forensics is a Latin word that means "to bring to the forum." And that's really what we're talking about when we say "computer forensics" -- bringing information about a computer-related incident to the court.

In essence, how do you take a computer that has:

- been a victim of a crime
- or facilitated a crime

and gather and formulate information from that computer in a way a legal court will understand?

Important: Today's technical tactics **may not** be acceptable in a U.S. court of law.

What does this mean?

You may be able to track down an attacker, but your methods may invalidate the evidence.

With new U.S. state laws (such as California Senate Bill 1386) making it mandatory for companies to disclose security breaches that compromise state residents' personal data:

- you may need to work with authorities to track down malicious attackers who have exposed you to liability
- but you need to make sure your methods of data gathering, collection, and storage will stand up to legal scrutiny.

How do you do this?

- Have good policy in place regarding your AUTHORITY to monitor and collect
- Pay attention to the MANNER in which you collect and store data

Collection and storage of data in the United States is governed by the Federal Rules of Evidence, which determine whether evidence is admissible or inadmissible.

"Regularly conducted business activity" is an important criterion because:

- If a monitoring activity is regularly conducted, it can create a record that can be used as evidence.
- If the monitoring activity is not regularly conducted, it may not be admissible as evidence.

Two other important principles:

- Chain of custody — every time data that has been collected is moved to a new location, this must be documented and recorded
- Authentication — the person who collected the data is the person who has to authenticate it in court (even if another expert then testifies about the relevance of the data)

An example of authentication: "If I, Rich Nolan, happen to be monitoring the logs and I observed that there was this type of attack in place and I hit the record button and I downloaded and collected the logs and I handed them off to my IT manager and then it went through the chain of command and ends up becoming an incident, later on at court I would be the one that would have to say, 'Yes, those log files that you have right here, whether they're electronic or printed out, are the ones that I recorded seven months ago in my lab.'"

Keep in mind: Any local jurisdiction may have local rules that also need to be considered.

This means, for example, that if you scan your networks daily for problems, this will be viewed as a regular business activity and likely can be used as evidence in case of any intrusion.

Takeaway point: AVOID ad hoc troubleshooting. It may be system administrators' first instinct to jump in and try to solve the problem — but doing so could invalidate evidence. Make sure you have regularly scheduled procedures to detect any anomalies.

PART 2: PUTTING IT INTO PRACTICE

So where should system administrators draw the line in their response to a potential incident? This can be tough. We need to teach system administrators how to be first responders. This means:

Start off in a very secure posture that WILL be admissible in court. Then:

- If it is a forensics issue, you can easily turn it over to law enforcement or other appropriate parties.
- If it turns out not to be a forensics issue, you can always de-escalate and begin troubleshooting.

NOTE: It is **extremely** difficult, if not impossible, to escalate to a more secure investigation posture once you've begun troubleshooting in an ad hoc manner.

Forensics often requires specialized equipment and training, so business leaders need to make sure their IT staff know when to seek outside assistance.

A response plan can accomplish this. The plan should describe a routine first responder procedure that is always used in dealing with incidents.

Through policy and regular training, make sure IT staff understand:

- what their limits are
- what they should do
- what they shouldn't do

Generally, IT staff should act to protect their network:

- stop damage from occurring
- stop information from leaking

- block attack traffic

Beyond that — for example, if considering tracking down an attacker — they should contact law enforcement.

How do you know who to contact?

Consider InfraGard: an FBI-sponsored organization that invites business leaders to meet with FBI agents, the U.S. Secret Service Electronic Crimes Task Force, and others **before any incidents have occurred**. This lays the groundwork for good communication during later incidents.

Takeaway point: Make forensics part of your security plan. State:

- How you collect information
- Why that information is collected
- Where you store information after it is collected
- What the chain of command is for various types of incidents
- What the procedures are for various types of incidents

Documenting these things in advance will help first responders avoid exceeding their authority. That's good for the business and the responder.

PART 3: FIRST STEPS AND RESOURCE POINTERS

First steps in establishing a forensics plan:

- Identify the sensitive data that you're trying to protect.
- Put methods and security systems in place to record data that is useful in protecting that sensitive data.

For example, banks are trying to protect money, so they have:

- Vault doors that lock and are on time-coded sequences — directly protect the sensitive asset
- Smooth countertops for recording fingerprints — indirectly protect the sensitive asset by recording data about threats to the sensitive asset (bank robbers)
- Cameras in place — indirectly protect the sensitive asset by recording data about threats to the sensitive asset (bank robbers)

The point is: Not only is there a lock on the door; there are methods in place to monitor anyone who gets through the lock. This is, in essence, defense-in-depth that implements a forensics plan.

Another example: a company in California that keeps customers' credit-card data. The plan may include:

- Making sure credit-card data is encrypted (direct protection)
- Making sure systems that store credit-card data are hardened against intrusions (direct protection)
- Making sure systems that store credit-card data have monitoring tools installed (indirect protection)

To put a forensics plan and capability in place, CEO-level buy-in is vital.

The best thing you can do is give your first responders clear, well-defined policies that are enforced and supported by management.

Resources

CERT First Responders Guide to Computer Forensics

FBI Laboratory: Computer Analysis and Response Team

NIST Computer Forensics Tool Testing Program

U.S. Secret Service Electronic Crimes Task Force