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

Computer Forensics for Business Leaders: Building Robust Policies and Processes

Key Message: Business leaders can play a key role in computer forensics by establishing strong policies and proactively testing to ensure those policies work in tough situations.

Executive Summary

Computer forensics is not a core competency for many businesses, but it is increasingly a requirement when a security incident occurs.

This means business leaders need to embrace their role as makers of high-level policy in the computer forensics process. The end goal is to make sure front-line staff members – and the organization as a whole – are ready to handle the unexpected.

In this podcast, Cal Waits, a member of the technical staff at CERT and co-author of the First Responders Guide to Computer Forensics, discusses the specifics and challenges of establishing robust, repeatable processes for incident investigation and computer forensics.

PART 1: WHY POLICY IS KEY

Proactive Preparation

How can business leaders give first responders the level of support they need to carry out successful incident investigations?

Preparation is key. Don't wait until a disaster occurs to make decisions. Instead:

- Discuss and determine guidelines up-front.
- Come to an understanding on how problems that arise should be resolved.

In all of this, the key role for the business leader is twofold:

- Understanding the need for policy.
- Driving creation of the policy.

This is not to say that the business leader must create the policy alone. People across the organization with different responsibilities, strengths, and technology expertise should be consulted to provide specifics. However, the business leader should serve as the driver and champion of the policy overall.

The alternative to a solid policy is a muddled response, which can mean:

- Nothing useful will be found out; or
- Things that are found out can't be used in any meaningful way as evidence.

Who should the business leader liaise with to construct a good policy?

1. The legal department, for input on the organization's legal obligations (for example, laws such as Sarbanes-Oxley or HIPAA (the Health Insurance Portability and Accountability Act) may govern conduct).
2. The IT department, to understand what technology the organization has in place.
3. Perhaps an outside consultant, to make sure nothing has been missed in a survey of assets, available technology, and protection mechanisms.

Using Rehearsals to Clarify Policy

Once a forensics policy is in place, rehearsals and simulations can play a key role. There are two types:

1. Tactical rehearsals, involving individual practice of skills such as gathering data or analyzing log files.
2. Large-scale rehearsals, involving group response to a simulated incident.

Large-scale rehearsals are vital, because they can illuminate breakdowns in processes *before* an incident occurs. Maybe the IT department isn't communicating with the legal department, for example, or the HR department doesn't know how to get involved when needed.

The time to find this out is not during an incident. It's during the rehearsal, when you can:

- Streamline processes.
- Find out where things aren't working and fix them.

Building on that, it's also important to have a **non-attribution policy** so that no one is reprimanded for mistakes they make during a rehearsal. Finding and correcting mistakes is the goal, so staff members should feel free to respond naturally, without fear of being scapegoated.

PART 2: THE COMPLEX REALITIES OF INVESTIGATIONS

Forensics as Fiduciary Duty

When using their employer's information systems, employees should understand that they have little to no privacy. And this should be stated in policy (and, for example, in logon banners).

Meanwhile, the organization's obligations to stakeholders are the same during a forensic investigation as during any normal operation – to protect those stakeholders' interests.

In fact, a forensic investigation is usually necessary because someone wasn't watching out for stakeholders' interests in the normal course of business!

Therefore, the investigation itself is important in looking out for their interests. The organization needs to find out:

- What was going on
- How to prevent it in the future
- How to correct anything that may have resulted from the unauthorized activity

Minimizing Investigation Impacts

Regarding the potential loss of time or resources due to an investigation, there are ways to conduct investigations with minimal impact.

A machine often can be imaged (a process of taking a snapshot of the current state of the machine) without taking it off-line. Then the image can be analyzed separately, while the original machine may:

- remain in service as is
- remain in service with its operating system and other software freshly reinstalled
- be replaced by a new machine

Investigators do need the ability and authority to gather information in a thorough manner – but this doesn't need to mean months, or even days, of headache or downtime. In essence, a balance is possible.

More Complex Investigations

What if an investigation gets more complex? There are several possible scenarios. For example, an organization may need to call in law enforcement for an incident that relates to national security or child pornography.

In many other situations, though, an organization may choose not to call in law enforcement right away or even at all. Why not?

- The organization has an advantage over law enforcement: They don't need to ask permission to do anything, because they already own the systems and the information.

- This can be especially beneficial when dealing with an incident that spans national boundaries. If an organization is multinational and owns all of the systems involved in the incident, it can likely investigate in various countries much more easily than law enforcement could.

If there are more than two parties involved (so the organization does NOT own all of the systems involved in the investigation), the investigation grows even more complex. Laws vary among countries, and it can be extremely difficult to figure out which laws apply and coordinate among various countries to resolve an incident.

Preparing for the Unexpected

If something completely unexpected or unanticipated by policy happens, some good guidelines are:

- Remember what the policy is. It is a guideline to help the organization respond in a particular situation. It is NOT intended to rigidly hold the organization to a specific course of action when that is clearly the *wrong* course of action.

- Keep in mind the letter versus the spirit of the policy. Understanding the difference allows creative response in tough and unanticipated situations.
- Arm personnel with a good grounding in the technology of digital forensics, and educate them as to what you expect from them, to get the best response in unexpected situations.

Resources

CERT Forensics Portal

Virtual Training Environment