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

IT Infrastructure: Tips for Navigating Tough Spots

Key Message: Organizations occasionally may need to redefine their IT infrastructures – but to succeed, they must be prepared to handle tricky situations.

Executive Summary

IT infrastructures need to evolve and change as business requirements evolve and change. Business processes that were once streamlined may become complex. Employee access levels that once made sense may no longer seem logical. New assets may be added to the infrastructure and are often documented poorly or not at all.

Occasionally, critical moments offer an opportunity to re-examine your IT infrastructure to ensure it is on track to support the business mission. For example, a company may merge with or acquire another organization. A new IT manager may be hired, only to discover that the organization's IT infrastructure is in bad shape. Or, a new company may want to create an IT infrastructure from scratch.

In all of these situations, tricky situations almost certainly will arise. In this podcast, Steve Huth, CERT's deputy director for operations, and Steve Kalinowski, CERT's IT manager, discuss their experiences dealing with these tough situations and offer advice for successfully navigating tough spots.

PART 1: MASTERING MERGER HAZARDS

Identifying and Analyzing Assets

In building a new IT infrastructure: *first, figure out what assets are involved*.

This is even tougher in a merger, where two existing IT infrastructures are involved. Sometimes, you don't know what assets your merger partner has.

The result: Your vulnerability to attack may change, and you might not even know it.

So, consider:

1. The class of information you have to share.
2. The mechanisms by which you share it.

Re-examining Business Processes

In fact, a merger and IT asset review can be an opportunity to step back and look at many things, especially your business processes. You may find:

- Over time, special cases may have prompted many additions to business processes. This can mean once-streamlined processes have become cumbersome.
- Valuable data is stored in several different places within the organization, which presents security challenges

View this asset and process examination as an opportunity to consolidate and streamline.

During a merger, IT personnel management can also be a significant issue.

IT staff members *on both sides of the merger* must be made aware of consolidated or streamlined business processes; otherwise, they each will operate as they did in the old organization. With IT architecture staff, this is a particularly thorny problem.

Reviewing Employee Access Levels

Another important but tricky step is to review employees' access. Examine how many IT staff members have system administrator access. Do they really need it to do their jobs?

BUT: Be careful. People can react badly to losing broader or higher levels of access and privilege.

Tips to avoid negative outcomes:

1. Emphasize that it's not a matter of trusting the employee as an individual. Instead, it's a matter of figuring out the role's required level of access. Perhaps the employee will become involved in a more interesting business process as a result of the redefinition.

2. *In advance of any role redefinition*, have an established policy that states, "When your role is changing, we're going to re-examine things." Then employees will view it as business as usual, rather than taking it personally.

3. Treat everyone equally, and lead by example. C-level executives should have their access reviewed as often and as thoroughly as junior staff members.

4. Additionally, high-level leaders and staff don't need total access "just because." They should have the access they need, and should have to go through regular channels to broaden that level of access.

5. If you have a good HR department, get them involved. Run your access-review plans past them and get their opinion on how people may react. You may decide to rethink your plans based on their input.

PART 2: WHAT TO DO WHEN YOU INHERIT TROUBLE

Listen First

What if you are hired by an organization and find that you have inherited a mess?

The best first step is to **listen**.

Avoid a bull-in-a-china-closet approach.

Instead, discuss the issues — not just with management, but also with folks in the trenches. People close to the action often know *why* messes exist *and are as upset about them as you are*.

If this is the case, you can approach the problem from a process-oriented viewpoint and attempt to improve those processes to help everyone adapt.

Resistance versus Deception

You may encounter resistance from employees at the outset. And here's a tricky part:

A malicious insider may behave similarly to an employee who is merely nervous about his job. For example, the insider may identify himself as a hero struggling against broken processes while also pushing back against some reforms. When you dig a little deeper, you find that he is trying to conceal malicious behavior.

One good way to tell the difference: Ask the person, several times if necessary, how you can make his situation better.

If he shuts you out every time you do this, it's possible that something underhanded is going on.

Change and Risk Management

Also, if you're handed a mess: Always put in place a good change management process.

Change without change management can introduce security vulnerabilities. Dependencies exist throughout organizations and are often poorly documented. If you change a router setting, for example, that may have been the organization's only line of defense against a particular threat.

So, first, figure out the dependencies. Then make changes from a knowledgeable place.

Keep in mind that resources are almost always scarce. A structured methodology may be useful in prioritizing actions.

One example is OCTAVE, a risk management framework. With OCTAVE, you can start small and work up to an organization-wide assessment, if you choose.

PART 3: BUSINESS-SIDE BUY-IN AND TONE FROM THE TOP

Bringing in the Business Side

To what degree should non-technical business leaders participate in IT infrastructure security actions?

Some tips:

Involve C-level executives early in the process to establish security rules based on business processes and assets. General operations and implementation then can be delegated in many cases.

If you're using OCTAVE, keep in mind that it requires a business perspective to identify the most critical assets. Business line executives and business unit leaders must be involved for this to work.

Policy Is Critical

Likewise, when working at the policy level, it's a good idea to have business leaders' perspectives.

The difficulties:

- Policy is hard.
- It takes a long time to do it right.
- There is no known silver bullet.

Policy is also an iterative process. There is no perfect policy for all time. Policies must change as the business changes, and this calls for ongoing review.

A merger or acquisition is a perfect example. Let's say a small organization is acquired by a larger one. Perhaps the small organization had never needed strict controls, but now it does, because a security breach in the small organization can provide an attacker with access to the larger organization's assets.

Getting Employees on Board

Just as employees may resist role redefinition, it also may be difficult to get them on board with policy changes. Some tips to avoid problems:

- Explain the big picture. Tell the employees that this is about helping the organization get to the next level.

Also, at a lower level, explain why the policy exists. Use scenarios to illustrate what might happen if the policy is not adhered to.

Keep in mind that we're all dealing with a business of people, not a business of machines.

Resources

CIO magazine

Information Security Forum's Standard of Good Practice for Information Security

ISO 17799

OCTAVE

Wood, Charles Cresson. Information Security Policies Made Easy, 10th Edition. Houston, Texas: Information Shield, May 2005.
