All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Reducing the Effects of Malicious Insiders Non-technologically

We hear a lot in the media and hype-cycle about “insider threats”, but most solutions we see offered in the marketplace are purely technical in nature. This article is about some other approaches to dealing with malicious individuals with insider access.

What is an insider threat?

Definitions being disputed seems to be part of the process of understanding any given issue. You can tell that “insider threat” is not a settled issue because of the ongoing debate over use of the term. Here's one definition:

> Insider threat := insider

Clearly, anyone with inside access (whatever that is) can be or become loyal to something other than the organization they are an insider within, and thus all insiders are insider threats.

We tend to talk about malicious insiders, or sometimes insiders behaving badly. The reason is that the accidental insider (any non-malicious insider), will produce errors and omissions. They will, on average, make more mistakes when tired, on Mondays and Fridays, and when under other sorts of stress. On an every-day basis, enterprises must deal with the natural imperfection of humans and everything else, because people aren't perfect.

Malicious insiders are, in our way of discussing these issues:

> People with inside access who intentionally act against the interests of the organization they work for.

This definition remains problematic, but we will adopt it nonetheless.

Who are they and why do they do it?

Many folks go directly from the definition of insider threats to their characteristics. We stop to do another level of differentiation. Here is part of our standard generic threat evaluation table. Threat types are associated with funding, size, motives, skill level, effort, and access.

Threat	*Funding/job*	*Size*	*Motives*	*Skill*	*Hrs/task*	*Access*
activists	10K	1-10K	Justice	Med	10K	Insider
consultants	0	1	Money	Med	No limit	Insider
spies	>1B	>10K	Patriotism	High	No limit	Insider
information warriors	>100M	1-10K	Patriotism	High	10K	Insider
insiders	1K	1-5	Money/Revenge	Med	1K	Insider
maintenance people	100	1-5	Money	Low	10	Insider
vendors	1K-1000K	1-20	Money	High	1K	Insider
whistle blowers	.	1	Justice	Low	100	Insider

Malicious insiders

Characteristically, insider access comes to those who have special knowledge of internal controls that are unavailable to the general public, and they have some amount of authorized access. In some cases, they perform only authorized actions, in terms of information and mechanism access. They are typically trusted, and those in control often trust them to the point where placing internal controls against bad acts are considered offensive.

To be clear, many of the technical attacks we hear of involve gaining inside access by bypassing controls. Many of these cases also involve exploiting non-malicious insiders in their normal behaviors, or taking control of system after system to form a sequence granting increasing access over time. This is not what we are talking about.

Malicious insiders either start interacting with the organization disloyal or turn from loyal to disloyal over time. While detecting turning behavior could notionally be detected by changes in behavior, those who start malicious and stay that way, presumably don't have substantial behavioral changes. I say presumably because, in fact, it's not all that clear. An intelligence operative, for example, might lay dormant for a time and then start to act maliciously.

Studies and what they have shown

There have been quite a few studies of malicious insiders and their characteristics. The Carnegie-Mellon CERT[1] has done and published a number of studies, and PERSEREC [2] has studies related issued for a long time in the context of eligibility for clearances and suitability for work. Other funded research has been done by government organizations over time and by some private companies, typically small consultancies or other specialists. Most of the studies we have seen started by collecting data on historical cases. Analysis was done of these cases to identify various items of interest to those studies. The net effect is, to a first approximation, the following seemingly interesting conclusions (mine not theirs):

- All of the results are based on insiders detected and caught, so nobody knows how many got away with things and were never detected. Longstanding estimates are that:
  - 1/3 of folks will steal if they think they can get away with it, 1/3 will steal even if they think they won't get away with it, and 1/3 won't steal regardless.
  - 2/3 of actual losses from malicious acts involve malicious acts by insiders.
- Malicious insiders tend to (~80% of the time) get detected by administrative and/or technical means several months before they do substantial harm.
  - Management response to detections is typically inadequate to stop the behavior, and that is what produces the ultimate substantial loss.
- Almost all such studies lack base rates for detection.
  - For example, even if 95% of all malicious insiders have coffee in the morning, that may also be true of non-malicious insiders.
  - As a results of the lack of base rates, detection based on results produced in these studies may produce large numbers of false positives resulting in “witch hunts” and similar things that may actually cause more insiders to change loyalty (i.e., turn).

1 Computer Emergency Response Team, which became a Federally Funded Research and Development Corporation (FFRDC) has several such studies published on its Web site.

2 The US Department of Defense Personnel Security Research Center

- Closely related phenomena, such as quitting behavior, have been studied, both in multiplayer gaming scenarios and in enterprises. Some commonly reported results are that those who are going to quit change communications behaviors:
  - They tend to go to job sites on their Web browsers
  - They tend to communicate less with other insiders in the work context until the last few weeks at which point they increase internal communications.
  - Their communicated content tends to be less positive as they approach quitting.

These may seem obvious to you, but many of these potential indicators are detectable. For example communicants behavior and Web browsing is detectable by purely technical means and automation to do this sort of analysis is currently entering the market.

What are the non-technological means?

This paper is really about the things you cannot do within computers, at least today. The most interesting of these seems to me to be the use of management to properly respond to what is already being detected by human and automated means. To get a sense of this, look at after-action reports and/or investigations of incidents like school shootings, military base shootings, workers changing companies en masse, executives leaving companies with internal information to start a new competitor, and so forth. We, and others tell us they, have seen a pattern of management not knowing or being directed how to respond to incidents.

- There is little value of getting information about potential future events if you cannot act on them to advance your objectives.
- On the other hand, without a lot of time and effort spent in studying the issues, it is unclear what actions management might reasonably take.

A scenario-based approach might help clarify the lack of clarity here

You are the CEO of company X. You have a staff of hundreds, including a CFO, CIO, COO, head of HR, head of Legal, head of Sales and marketing, and each has the usual staff, executives, workers, and so forth.

In Q1 of this year, you find out that 8 instances of password use from external unidentified systems were used to access internal information in Q4 of last year. All of the people involved indicate no knowledge of how it happened, seem upset by it, seem worried about being fired, and are told that password guessing and theft happen, are given a new password, trained on keeping them safe, and company X moves on.

Would you do anything differently? If so, what?

In Q2 of this year, you find out that 4 instances of storing internal data from databases on a public cloud (dropbox or similar service) server were detected by IT. Interviews with the people responsible indicated that they were each doing so in order to perform some legitimate function from home and had no other way to access the database from home. IT confirmed that policy didn't provide for this sort of access and the current technology didn't support it. As a result, workers were told not to do this any more and were told that they could request such data from IT and it would be provided in an authorized way if management approved.

Would you do anything differently? If so, what?

In Q3 of this year, you find out about various personal affairs between workers and executives as a side effect of an investigation of an unrelated matter. You express to the investigative lead that the details are private matters and outside of the bounds of what the business should be told. HR is instructed to make clear the sexual harassment issues associated with such affairs but to do so as part of normal HR training and not identify any particular incidents.

Would you do anything differently? If so, what?

In Q4 of this year, you find out that a high level sales executive who was having an affair with a high-level purchasing specialist used the now authorized process to exfiltrate both internal customer information (e.g., who they are, what they are charged for what, their contact details, personal likes and dislikes, names, addresses, contact details, buying thresholds, and so forth) and all of the internal cost information (e.g., what you but from whom at what price with what discounts, the contact details, personal likes and dislikes, and so forth). You find this out because they started a new company that is directly competitive, hired key people, and are selling the same products and services into the same customer base at better discounts. In the 2 months since they quit (at the end of Q3) they have taken away 20% of the business you had in the pipeline and are on a path to take another 25% in the next month.

This is not a made up scenario

In fact, this is a fairly common scenario for insider malicious insiders. All of the signs were there, if you would have looked for them, but even if you suspected this might be happening, what would you do about it and how would you bake this into policy, procedures, and process within your company? Here's what else you likely would have found if you were looking for it:

- You might have identified that one of the same people with a “stolen” password in Q1 was also a person who sent data to the cloud storage provider in Q2. Actually, their boss was aware of both of these, but had no specific requirement to act on it, and felt that this employee was a critical team member just trying to get the job done by working hard from home.
- You might have identified that one of the executives having the affair was the a sales executive who was having an affair with the same purchasing specialist.
- You might have identified that the sales executive was also authorized to send data out of the company using a cloud provider and was part of the team who supported the new method to legitimize this activity.

You might have found all sorts of other things out if you had investigated further, but that's not the point. The point is...

What would you do differently knowing this?

Chances are, at least today, nothing. Consider that almost any step you take to address the changing situation over time may result in legal action against you or your company, may end up making the problem worse, may end up losing some of your key people, and being heavy handed about these things might produce more people who jump ship to go to the new competitor.

A big part of the problem lies not with you or your company, but with the nature of our understanding of these issues as executives.

How should we change our understanding?

I have found some things to be true of people and business relationships. You may have found the same things. Here are some of my thoughts...

- First impressions are often predictive of future behavior.
  - Example: A company that doesn't want terms with penalties for late payments is likely to make payments late. If they start to do so, they will continue to do so.
- When people seem to back away and go silent, they are considering turning.
  - Example: A team member doesn't return calls or emails for a week or more after having regularly scheduled meetings. They are likely backing out of the team.
- People who seem too valuable to fire and take advantage of that are often disloyal.
  - Example: An employee repeatedly does unauthorized things to exfiltrate or alter content adapting to changing rules. They are likely malicious.

All of these things seem sensible but have very limited basis in fact

My experience could be completely wrong and cause legal problems

None of these examples tell managers what to do about it and when

If you are going to address this issue, you need to have a pre-defined understanding and likely a formally written approach to dealing with these issues.

The problem is not in our stars...

It is in our research – or rather, the lack thereof. Plenty of research is done into technical aspects of “insider” detection and defense. Even though most of this work fails to differentiate between malicious and non-malicious insider acts and fails to address base rates, at least it is being done. But where we are not doing research and continue to ignore the historical events and research is in the area of human resources, management practices, and making decisions about how to deal with people behaving in undesired ways.

My initial guesstimates base don historical results are no substitute for the hard work required to understand the nature of people and how to manage them. It's not an easy problem, and perhaps hard to convince management to fund. But it must be done if we are to make progress in this area.

Summary

We know a great deal about insiders behaving badly and what they tend to do. But what is almost universally missing is a defined regimen for handling personnel issues that deals effectively with this issue. In order to produce such a regimen and have it operate effectively, we also need something else we are missing – sound research.

