FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

How to Mitigate the Risk of Insider Threats

By Dan Geer

The Age Of The Insider Threat

With lines like "If neither foes nor loving friends can hurt you," Rudyard Kipling's bracing poem "If" challenges the reader to face uncertainties, including the uncertainty of never knowing where a threat can come from. The WikiLeaks saga does the same.

The calculus of threat is the probability of an event's occurence times the downside consequence if it does occur. An insider attack may well be rare, but because data is an increasing fraction of total corporate wealth, the consequence of an insider attack on the corporation's data grows as fast as the value of that data grows.

And in a fully connected world, there are no private tragedies. A growing body of civil law demands the public shaming of any corporation that leaks other people's data. The body of financial regulation already in place is beginning to treat data loss events as inherently material, thereby elevating such matters to the Boardroom level, per se. On the very day this is being written, designers of national policy are announcing proposals to make protection against insider attack within the officially designated critical infrastructure a mandate that includes a periodic inspection regime.

Insider threat has truly come of age.

Approaches To Mitigating The Risk of Insider Threat

An insider, to be an insider, must already have passed through an access control gate. Therefore, access control is not a deterrent to insider threat. An insider, to do his or her job, must have authorization credentials congruent with the task they must do. Therefore, authorization systems are not deterrents to insider threat, though they may bound the downside consequence to a degree. Some members of staff must have special authority simply because keeping the IT plant running will always require unanticipatable interventions when parts fail. Such special authorities may also be available to any internal investigations team that may be in place, and similiarly to any internal Red Team.

In other words, there will always be persons in positions particularly capable of being an insider threat. That is not bad, but it is a reality. The question is how to control this by some means that is not itself subject to the very access control, authorization, and legitimate capabilities of the determined and knowledgable insider.

The answer is that the operating environment itself must be altered. Of all possible design goals for any security system, perhaps the highest is "No silent failure." If we must alter the operating environment in a manner consistent with preventing the silent failure of an expert insider attack, the engineering problem is at least well specified.

The most cost-effective solution to this engineering problem is to instrument the operating environment such that data does not move without that movement being observed by the instrumentation. The transition from data-at-rest to data-in-motion always involves the operating environment and does so in a way that is directly subject to instrumentation. That instrumentation is difficult to do without side effects is a given. That that instrumentation — that event-detection scheme — implies the existence of a mechanism to receive and act on the detected data events in real time is likewise a given.

For maximum practical utility, the mechanism that receives and acts on the detected data events needs to be adaptive. The operator may well want to know about data events that do not require intervention, only surveillance. The operator may well want to take actions the logic of which involves not only the data event but other externalities, such as time of day and geo-location. The operator may need to have different rules when the entire environment is diminished, such as by extreme weather events. And so forth.

About Digital Guardian

At Fortra™'s Digital Guardian®, we believe in data. We know that within your data are your company's most valuable assets. The sum total of innovations, plans and potential. We protect your company's sensitive information like it's our own so you can minimize risk without diminishing returns.

For over 10 years we've enabled data-rich organizations to prevent data loss at the endpoint. Our expert security team and proven Digital Guardian platform radically improve your defense against insider and outsider threats.

Hundreds of customers across a wide range of industries rely on Digital Guardian to protect their critical information at the point of risk. Seven of the top ten IP holders and five of the top ten auto companies trust us with the integrity of their most valuable and vulnerable data. We take pride in knowing that, at this very moment, Digital Guardian agents are securing the sensitive data of the world's most inventive, influential companies.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.