2006-06
Why the CISO should work for the CEO
- Three Case Studies -

Introduction:

These three case studies show why we think Chief Information Security Officers (CISOs) should work for the Chief Executive Officers (CEOs). The situations are real and recent – the names are concealed to protect the shareholders.

Case Study 1: The Unreported Incident

The CISO of a major enterprise was not informed of a major incident that information operations knew to be underway. After discovering it during investigation of a major global outage, the CISO decided to ask information operations to take substantial action to mitigate the risk on an urgent basis. The request was reflected in notices sent out of pending changes, and seeming action, but four weeks later, another similar incident occurred and the CISO found that the fixes had not been done, producing another major outage.

An urgent meeting was called with the CIO, who both the chief of information operations and the CISO worked for. In this meeting, the chief of operations said he had ignored the urgent request because it would take too long and be too hard to do. The CISO again expressed the criticality of the issue by explaining that even as they spoke an incident was underway, that it was resulting in work stoppages, and that increasing numbers of longer, more frequent, and more intense incidents would almost certainly be seen until mitigation was completed. The CIO decided that rather than focus or spend money on urgent fixes, a strategic project would be started to mitigate some time in the next quarter.

As I write this, information is being stolen from this company, their network is infested with many viruses, weekly outages are close at hand, the shareholders are losing value, and the CEO hasn't got a clue. It's the CEO's fault for not realizing that direct CISO reporting to the CEO and independence from the CIO are fundamental and necessary for success against risks from information attacks and information technology failures.

Case Study 2: The CIO no longer

This CIO was in charge of the CISO and their information protection program. But when an external assessment was ordered from above, the CIO found out just what being in charge means. Rather than have a separation of duties and independent experts in key security positions, this CIO had systematically weakened the information protection program and invested in a $200M data center consolidation project. The only problem was that security was left out.

The CISO knew of the problem of not baking in the security and had gently requested the ability to review and opine, but the CIO kept the CISO out of it. They devices an ISO-17799 based policy, but it had two problems; (1) it was just a copy of ISO replacing a few words like “organization” with the name of the organization, which means it was never really read, understood, and considered, and (2) they didn't implement any of the things they put in the policy. As the project started to go over budget and they couldn't figure out how to get it safe enough to deploy, they found out that their single data center had been put in a flood plane off the end of an airport runway without adequate power redundancy and with no perimeter. That CIO is now “retired”.

Case Study 3: A $60M loss

This CIO wanted the data center consolidation because it reduced cost and increased efficiency. Clearly a laudable goal and one that any enterprise would applaud, if it weren't for a minor problem. When the consolidation happened, the CISO was shunted to the side by the CIO. As the effort was well underway, an outside protection review found what a near-death experience clearly demonstrated.

The effort to reduce cost when too far and eliminated the redundancy that was key to assuring business continuity. A subsequent disk failure in a mainframe caused an outage that cost the enterprise about $50M in direct losses. The replacement of the redundancy on an urgent basis cost the enterprise another $10M. Shunting of the CISO by the CIO was a bad move, and one that cost this large enterprise a significant part of its profits for the year and cost its shareholders more than a billion dollars of reduced share value for a year or more.

Conclusions:

The CISO can only be ignored or shunted when they are under control of someone who wants it that way. We do not question the intentions of the CIOs in these three case studies. The fact is that most CIOs don't understand the risks they take on behalf of their enterprises and don't listen to warnings from CISOs who work for them. We can't guarantee that a CEO will listen either, but it is the CEO's job to manage enterprise-level risks and they cannot manage what they cannot measure. Measuring information-related risks means direct CISO reporting.

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 18, section 2.3.4.5 we present:

"Resale or Theft of Company Inventory"

> *"In this one the perpetrator sells company inventory for cash and the company records the goods as stolen for a loss. They may also commit insurance fraud along the way by trying to get an insurance company to pay for it, which is why insurance companies tend to investigate such things as possible frauds."*

A recent case that didn't make the news involved a network administrator who seemed a bit too protective of his storage space when the auditors came around. He was backed up by the CIO who told the auditors to respect his privacy (even though they are the company's assets – or they were supposed to be). The auditors got curious, as auditors do, so they wrote in their audit report that the matter should be investigated. This produced unhappy top management who asked for it to be removed. And so it was, when they called in the police to investigate the theft of tens of millions of dollars in network hardware. In this case the thief didn't have the chance to get the equipment "stolen".

Chet's Corner

It's tough being me, but some months things just seem to work out. Last month I gave four "Lunch and Learn" sessions at the CompUSA in Omaha, and every one was overflowing. I started work on a three-month contract with a large software manufacturer, got a contract with a major telephone company to start providing virus defenses and other services, and started working on wireless for a well-known non-profit. I got paid on time, I took a day off each week, and things are starting to click.

Was everything perfect? Of course not. But as the song from "Life of Brian" goes:

"Always look on the bright side of life"!

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's forensics:

A recent case for more than $10M got settled out of court to the great benefit of one of our clients based, at least in part, on our expertise with data extraction from floundering media.

In this case, a floppy disk from about 15 years ago was the only evidence of the sequence of events that took place, and it proved unreadable to others. So in a fit of desperation, they contacted us.

It took about $40,000 of effort by the time we were done, but we got all of the bits off of that floppy and were able to provide all parties with the key evidence they needed to determine more definitively what happened when and who did what.

> Our first expert report included the contents of the floppy and a detailed description of how we extracted it and why it accurately reflects the bits last written on the disk.
>
> The second report responded to an implication of a possible forgery. It detailed error modes that could have caused the errors found, mechanisms that could more definitively determine when the disk was actually written based on the details of the error mechanisms, and an opinion regarding the potential for forgery based on the available information and what it would take to definitively prove the matter one way or the other.

Digital forensics is sometimes expensive, complex, and time consuming, especially when you deal with the hard cases and a lot is at stake. Sometimes it takes a Ph.D. to get to the truth of a matter.

Mollie gets the last word in

My name is Mollie, and I am the editor of this monthly. This month I packed up my things and moved back to Livermore for the summer to get this project rolling. It's in its infancy, but before I finish with it, it will be at least a teenager! Have a great summer.