Data pirates

M. Simon, Technical Contributor

 As if we didn't have enough to worry about with government tracking and collecting information [1] on our every move, we also have to be on the lookout for data pirates. Although, if the pirates get their hands on the government databases, the problem begins to look like a single problem with diverse parts.

We do load up with protections against intrusions into our home and corporate networks. We have Norton, Malware Bytes, Spybot, and a host of other protectors to keep our network safe from outside infiltrators. But that is not where the biggest vulnerabilities lie. The biggest threats are from insiders. People we trust. When data was in file folders and indexed with card indexes, the sheer mass and bulk gave us some protection. Even the theft of a few pounds of computer printouts limited to some extent the amount of data that could be purloined. Except for dumpster diving. Which was then countered by shredding and double shredding. But now we have USB flash drives. And 64 GB drives are available. With bigger ones on the way. That is a lot of data in your shirt pocket.

The Data Administrator Newsletter [2] lays out the threat.

> *...it's precisely due to our investment in layers of security that the threat of intrusion is so relatively small. The intrusion threat is very real, and if we weren't so well prepared, break-ins would in fact be one of the biggest piracy threats, especially considering the high value of our data to competitors and others. So we definitely need to be spending big to protect against potential unknown intruders.*
>
> *But assuming we've addressed this area adequately, the threat from outsiders is most likely under reasonable control. So what's left? Where is the danger coming from?*
>
> *We can find out by reading the stories behind the headlines above. In every case, the threat came from insiders: employees, former employees,*

> *individual contractors, employees of corporate contractors, and so forth. Insiders are the hole in the security cheese.*

The newsletter then goes into all the laws **YOU** can break if someone steals data from you. And that does not even count the loss of trust from your most valuable resource: your customers.

What can you do? The first thing is partitioning. What the military calls "need to know". Then, you watch who accesses the information. How much do they get at a time? In what form? Are they getting specific records or digests? A digest being things like "how many customers bought widget X59"? There are vulnerabilities to information in digest form. Industrial espionage is not unknown. But it does not break the trust of customers.

What can you do? Well, that is hard to figure out. Especially if you have a dedicated thief who is smart and has the trust of the organization. The Dixon Illinois Comptroller who stole $53 million [3] over a period of years proves that. But money will be noticed eventually if there is enough of it. Careful data thieves who don't use the data in an overt way could get away with such theft indefinitely. Maybe they just pick off customers here and there. A few at a time. Or advertize to them a related product in a targeted marketing kind of way.

The only advice I can offer (and it is not sure-fire by any means): Be careful out there.

M. Simon's e-mail can be found on the sidebar at Space-Time Productions [4].

Engineering is the art of making what you want from what you can get at a profit.

Links:
[1] http://www.deseretnews.com/article/865577495/ACLU-concerned-about-background-check-in-gun-bill.html
[2] http://www.tdan.com/view-articles/5283
[3] http://www.huffingtonpost.com/2013/02/14/rita-crundwell-sentencing_0_n_2685121.html
[4] http://spacetimepro.blogspot.com/