

Re: Notebook policy (need advice)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-01/msg00361.html>

- *From:* "Eric Furman" <ericfurman@xxxxxxxxxxxxx>
 - *Date:* Fri, 26 Jan 2007 15:19:12 -0500
-

What would you do if you found out an employee was routinely walking out of the office with hundreds of thousands of dollars of company money in cash? He wasn't stealing it. Never mind the preposterous nature of this scenario, because in effect, this is exactly what people are doing when they walk around with a laptop with sensitive data that if it were compromised could cost the company this much money and oh so much more. You would think it was insane and can whoever it was, on the spot. Up to and including a CEO (removed by the board, in this case). I used to work for a "Very Large Bank" and this was exactly the policy.

On Fri, 26 Jan 2007 13:58:22 -0600, "Eric White" <ewhite@xxxxxxxxxxxxx> said:

So you don't really mean:

Anybody, and I mean ANYBODY, found with sensitive data on their laptop should have it seized and they should be immediately dismissed.

Eric Furman wrote:

Oh please, this is hardly worth replying to.
Said laptop would be in the possession of an armed law enforcement official. Hardly an unsecure environment.
Thanks for playing, try again.

On Fri, 26 Jan 2007 09:09:49 -0700, "Patton Roub" <proub@xxxxxxxxxxxxx> said:

What would be your recommendation to the drug enforcement Special Agent who is recording the sensitive data outside the house of a suspect, and then using that data to create a search warrant on that computer to present to a Judge down the street? Oh, did I mention the data he must have downloaded earlier to make sure he is looking for the right guy?

Re: Notebook policy (need advice)

Wireless is not available, and we don't want Special Agents climbing poles.

Never ever say never.

Regards

Patton J Roub

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx

[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]

On Behalf Of Eric Furman

Sent: Thursday, January 25, 2007 2:09 PM

To: security-basics@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Subject: RE: Notebook policy (need advice)

I'll give you one very simple policy that you should enforce that will make most of your concerns moot:

NEVER EVER EVER STORE SENSITIVE DATA ON A LAPTOP!

Anybody, and I mean ANYBODY, found with sensitive data on their laptop should have it seized and they should be immediately dismissed.

There is virtually no reason to ever store sensitive data on a laptop. Sensitive data should only ever reside on hardened servers in a physically secured server room. If your employees need to work with this data there are several means to securely access this data remotely.

(And, indeed, make sure the room AND its data storage is truly secure. There have been recent break-ins at certain companies and data tapes containing sensitive data were stolen.)

On Wed, 24 Jan 2007 22:50:47 -0500, "Tony UcedaVélez" <tonyuv@xxxxxxxxxxxxxxxx> said:

Re: Notebook policy (need advice)

Definitely agree with the previously made comments on the use of full disk encryption and points made on AV, however, I wanted to simply add to those points by saying that the issuance of notebooks should be focused on those user groups that would most benefit from a portable computing device.

Not all positions within a company require the use of a notebook for work (although, in the near future this may very well change). Obviously, the portability of laptops could be recommended to be reserved for those who travel/ telecommute or use it for working sessions in company war rooms (developers, project managers come to mind). Point here is that the scope and applicability of any security policy could achieve a more targeted audience, versus a broad unknown audience who truly don't benefit by having a notebook.

This recommendation is obviously touch to act upon in organization's where notebooks have already been issued without specific consideration to the job function. However, if possible the added value in the above mentioned is the following:

1. IT Operations adheres to imaging and providing laptops to those whose roles and responsibilities require the use of a notebook. Often times, IT Ops groups elect to image a resource that is readily available or one in which the user prefers.
2. Again, a policy surrounding notebook usage will be geared to a specific audience instead of rolling out a policy to

Re: Notebook policy (need advice)

everyone, regardless of whether they have a notebook or not. Improved accountability, focused security CBT modules (related to mobile computing) are some positive by-products that result.
3. Cost savings can be multi-fold here. Since roles and responsibilities will dictate who gets a notebook, cost savings are realized not only on the price per notebook, but also the costs associated with software licenses that are specific to portable information assets.

Again, this suggestive advice obviously depends on the 'mobile' culture of your company's workforce. Also affecting the above is whether you'll be able to 'backtrack' to make such a recommendation.

Regarding local admin use, again, I would revert to what the roles and responsibilities are for the employees and creating various images that coincide with their respective user groups/types. Ideally, a collaborative effort between HR and IT Security should make this work.

Btw, along with AV and FDE, I'd include in the policy the use of personal firewalls and HIPS agents, especially for the road warriors of your organization.

Hope this helps.

Best Regards,

Tony UcedaVélez, CISA, GIAC
VerSprite, LLC
(office) 678.938.3434
(email) tonyuv@xxxxxxxxxxxxxx
(web) www.versprite.com

Re: Notebook policy (need advice)

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx
[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]

On Behalf Of Nicolas Arias

Sent: Tuesday, January 23, 2007 8:12 AM

To:

security-basics@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Subject: Notebook policy (need advice)

Hi guys!, in my company we have a lot of notebooks, but theres no formal security policy about them.

Can you tell me how do you handle this?

Do you give an local admin for the owner?, do you use full disk encryption?, what about anti-virus and external scans?

Any idea is going to be really preciated.

Cheers!!

--

Eric White ewhite@xxxxxxxxxxxxx