



## MAGAZINE

[Subscribe & Get a Bonus CD](#)  
[Digital Edition](#)  
[Customer Service](#)[Research Directory](#)

<a href="#">Software &amp; Services</a>	<a href="#">Office Hardware</a>	<a href="#">Security</a>	<a href="#">Servers &amp; Storage</a>	<a href="#">Cell Phones &amp; Mobile</a>	<a href="#">Operating Systems</a>	<a href="#">Networking &amp; VOIP</a>	<a href="#">Virtualization</a>
---	---------------------------------	--------------------------	---------------------------------------	--	-----------------------------------	---------------------------------------	--------------------------------

Sign in with  or [Create a New Account.](#)

## Security Alert

Practical security advice » [More Security Alert](#) » [RSS](#) » [All Blogs](#)[Like](#) 37K

@pcworld

Enter your email to get BizFeed newsletter

Recommend: [Like](#) 115  52  0  185  [Email](#) [9 Comments](#) [Print](#)

BUSINESS CENTER Feb 21, 2011 1:23 am

# Lessons Learned Thanks to HBGary and Anonymous

By [Tony Bradley, PCWorld](#)

A week or so ago, I had never heard of HBGary. I assume you probably hadn't either. Now we know HBGary all too well after an attempt to make a name by unmasking the anonymous hackers of Anonymous [backfired in more ways than one](#).

## SIMILAR ARTICLES:

[8 Security Tips from the HBGary Hack](#)[British Police Nab Men Believed Linked to HBGary Data Breach](#)[FBI Steps Up Hunt for LulzSec](#)[It's a Hoax: Anonymous Did Not Threaten Westboro Baptist Church](#)[7 Ways to Avoid Getting Hacked by Anonymous](#)[Your New Facebook Friend Might Be A Spy](#)

Anonymous has become a virtual household name following the group's "hacktivism" against companies and Web sites that made efforts to knock Wikileaks offline and [cut off Wikileaks' funding](#). The activities conducted by Anonymous were illegal, but to many the attacks were a heroic defense of disclosure and the freedom of speech. Anonymous has since embraced this role as Robin Hood of the Internet and has continued striking new targets-- recently threatening to [take down Westboro Baptist Church](#) and its site godhatesfags.com. It's hard not to like them.

Then, HBGary—a small Sacramento-based security firm—claimed to know the true identities of the leaders behind

Anonymous, and threatened to reveal them. Anonymous did not appreciate the threat, so within a matter of hours it hacked and defaced the HBGary Web site, and compromised its servers. Tens of thousands of HBGary e-mails were then exposed on the Web, and that is where HBGary's problems begin.

As if getting pwn3d by Anonymous and having sensitive information compromised wasn't bad enough, the content of the exposed e-mails uncovered a larger scandal involving an HBGary affiliate--HBGary Federal. Apparently, HBGary Federal was involved in an ethically dubious plan to use fake social networking profiles to discredit groups that criticize the US Chamber of Commerce.

So, what pearls of wisdom can we derive from this sordid tale? Well, first, that locking down servers and protecting data is a complex and difficult task. HBGary is an information security firm—implying some higher than average understanding of information security--and it was hacked in a matter of hours.



## Buying Guide



Routers and Wireless Adapters: Here's how to choose the equipment you need.  
[Read more.](#)

## Business News Daily

Get the latest technology news that's important to you and your business, fresh seven days a week.

Enter e-mail address

## Best Prices on Backup Utilities

[MOST POPULAR](#)[ALL CATEGORIES](#)

Second, this incident demonstrates that [skilled hackers are a formidable force](#). There are tons of script-kiddy bad guys out there who use automated tools and don't really know how to hack. But, for an attacker with real skill, security measures are more like speed bumps than steel walls--breaking or circumventing them is more a matter of when than if.

Third, we learn that sometimes there is a fine line between the good guys and the bad guys. Ostensibly, the two have roughly the same skill set and all that truly separates them are ethics and some sort of moral code. Lacking that, there is nothing stopping an otherwise legitimate security professional from using his skills for evil rather than--or in addition to--good.

For the first two lessons, IT admins need to understand that there are no silver bullets, and that there is never a point where you are "done" [securing the network and data](#). You must implement a layered defense of reasonable security controls, then diligently monitor for threats and suspicious activities 24/7.

As for the third lesson, make sure you do your due diligence before doing business with a security consultant or hiring a security firm. Do your best to make sure you are doing business with someone with the skills necessary to get the job done, and the moral compass to not cross the line.

WAS THIS ARTICLE USEFUL? [Yes](#) 78 [No](#) 7

Sponsored Resource: [Do-it-yourself guide to home networking](#).

Read more like this: [hackers, network security](#)



You can follow Tony on his [Facebook page](#), his [Google+ profile](#), or contact him by email at [tony\\_bradley@pcworld.com](mailto:tony_bradley@pcworld.com). He also tweets as [@TheTonyBradley](#).

#### Sponsored Links

##### Antivirus Utility

Top Malware Removal - Free Scan Today - Download now!  
[www.pctools.com](http://www.pctools.com)

##### Sprint™ Official Site

First Moves Us Forward. Stay Ahead W/ Sprint 4G. Buy HTC EVO™ 4G Now!  
[www.sprint.com/First](http://www.sprint.com/First)

##### Shop iPad Cases

Uniquely styled iPad cases. All reasonably priced.  
[BoxWave.com](http://BoxWave.com)

##### Policy Procedure Software

Web-based Policy Software For Organizations. Try It For Free!  
[www.policytech.com](http://www.policytech.com)

## Comments Readers reply with their ideas and expertise.

SUBSCRIBE TO THIS DISCUSSION VIA [EMAIL](#) OR [RSS](#)



*Leave a comment*

Submit Comment

Once you click submit you will be asked to sign in or register an account if you are not already a member.

**MatthewScott** posted Mon Feb 21 00:29:01 PST 2011

plz do research before posting articles. Anonymous is not fighting WBC. k thx bai.

<http://anonnews.org/?p=press&a=item&i=494>

**BevRobb** posted Mon Feb 21 01:37:06 PST 2011

Hi Tony,

Thanks for another great article! I personally like reading between the lines in "the third lesson."

BTW, I received a few DM's on twitter today that Anonymous did not threaten to take down Westboro Baptist Church. One of the links I received is the same link that Matthew posted



**Norton Ghost v.15.0 (Full Product)**  
\$27.99 and up [See All Prices](#)



**True Image Home 2011**  
\$48.99 and up [See All Prices](#)



**Norton Ghost 15 (Full Product)**  
\$28.99 and up [See All Prices](#)



**Backup Exec 2010 for Windows Small Business Server with 1 Year Essential Support**  
\$346.23 and up [See All Prices](#)

[See all Best Prices on Backup Utilities »](#)  
See also:

### Latest in Business Center Blogs

**LINUX LINE** - OCTOBER 03, 2011 11:27 AM

#### [Excited for Ubuntu Linux 11.10? The Official Countdown Has Begun](#)

Promising 'a whole new world,' a dedicated site is now building anticipation and counting down the seconds until next week's release of 'Oneiric Ocelot.'

**SIMPLY BUSINESS** - OCTOBER 03, 2011 7:52 AM

#### [Free Workrave Utility Helps You Fend Off Repetitive-Strain Injuries](#)

Too much time at a PC can wreak havoc on your joints and muscles. This handy helper reminds you to take breaks at regular intervals.

**NET WORK** - SEPTEMBER 30, 2011 5:54 PM

#### [Windows Phone 7, Day 24: Find Your Lost or Stolen "Mango"](#)

I've been lucky enough to never have a lost or stolen smartphone, but it's nice to know if I ever do Windows Phone 7.5 "Mango" can help me find it.

**BIZFEED** - SEPTEMBER 30, 2011 5:05 PM

#### [Xobni Makes Gmail and Android Contacts 'Smarter'](#)

Xobni's contact manager revolutionized Outlook inboxes. Now it offers an inbox organizer that Gmail has been begging for, and a superior contact manager for Android devices.

**LINUX LINE** - SEPTEMBER 30, 2011 4:55 PM

#### [How to Land a Linux Job](#)

It's a candidate's market for Linux skills today. Here's how to put your best foot forward.

**BIZFEED** - SEPTEMBER 30, 2011 4:12 PM

#### [Google Offers Real-Time Site Analytics](#)

Businesses can now check out their Web statistics in real time with Google Analytics. Here's how this and the new Analytics Premium will help your business.

[All Blogs »](#)

### Featured Webcasts



#### [Top 10 Concerns of Buying a VoIP Business Phone System](#)

**Type:** whitepaper  
**Company:** CompareBusinessProducts.com  
**Categories:** VOIP



#### [Buying a Phone System? Compare the 94 Business Phone Systems in One](#)

above: <http://anonnews.org/?p=press&a=item&i=494>

Cheers!

Teksquisite (Twitter)

[Chart](#)

Type: w hitepaper  
Company: CompareBusinessProducts.com  
Categories: VOIP

[More webcasts »](#)

---

**tonybradley posted Mon Feb 21 06:20:33 PST 2011**

I love commenters who assume that because a tidbit of information that didn't exist when the article was written now exists, it somehow implies that the article wasn't "researched".

The Anonymous press release from the link was published yesterday. There is no time stamp I can see, so for all I know it was published **after** I wrote this article.

I think the WBC hoax adds an interesting twist. It will be interesting to learn who initiated the hoax and why. I also appreciate the part of the Anonymous press release where they reiterate the right to free speech--even when that free speech is vile and objectionable.

But, now that the quantlet was thrown, I wouldn't be surprised to see WBC get taken down--even if its by an Anonymous copycat.

---

**dagamer34 posted Mon Feb 21 06:28:22 PST 2011**

What did we learn?

"Don't poke the bear".

---

**DecentDiscourse1 posted Mon Feb 21 07:28:02 PST 2011**

Fact errors abound: "Then, HBGary--a small Sacramento-based security firm--claimed to know the true identities of the leaders behind Anonymous" No, it was HBGary Federal in Washington DC, of which HBGary of Sacramento had a 15% stake. Aaron Barr = HBGary Federal. Greg Hoglund = HBGary. Aaron had the dubious plans, Greg had the dubious tools in a war chest of zero day exploits. Also, you cannot conclude from the attack that protection is a "complex and difficult task" when it has been shown that principles of HBGary Federal re-used simple passwords on multiple systems, when lack of training allowed a 16 year old girl to social engineer new privileges out of HBGary's network admin and when HBGary fielded a fatally flawed CMS containing a common, well known security hole. Nothing complex or difficult about preventing any of the above.

---

**DamOTclease2 posted Mon Feb 21 10:56:02 PST 2011**

The article does not even begin to address the lessons learned. First and foremost we have learned that HBGary is **not** a "security company." We also have learned that the moron Aaron Barr is **not** a "security expert." We have learned that the U. S. federal government was taken in and swindled by these HBGary wannabe clowns for an undisclosed amount of money for HBGary's dubious services.

We have also learned once again that the fascists who work against Democracy continue to have government funding while the good guys (that would be Anonymous) continues to have the forced of good on their side.

---

**MarcusAureliusMccoy posted Sat Mar 12 09:53:00 PST 2011**

This story has a lot of the situation wrong. These guys are not Robbin Hoods and they will go down for extortion and assault and in all probability internet terrorism as well as spying. But the media has their proverbial head up where the sun don't shine as usual and in this instance are helping petty criminals, the one who infect your machines also. Seems like these sunspots have decreased humanity intelligence about 50% and its most prevalent listening to the above verbiage. In the end this kids will probably end up in jail and some of them will die and that will be due to stories like the above one which will only drive them harder to their deaths.

---

**nonseq** posted Sat Mar 12 10:30:33 PST 2011

**DamOTclese2** said

*We have also learned once again that the fascists who work against Democracy continue to have government funding while the good guys (that would be Anonymous) continues to have the forced of good on their side.*

Quis custodiet ipsos custodes?

**candive** posted Mon Apr 25 08:55:11 PDT 2011

Finally a Watch Dog / Attack Dog with the skill set required to expose the corruption.

Anonymous and Wikileaks I wish I had the skills to help your cause.

Very Sincerely

A True Canadian.

## Free Whitepapers



## Software and Services Whitepapers from PCWorld

[The Fastest Way to a Drupal Site](#)

[Gen Y Will Impact Your Future Growth. Report Shows How.](#)

[Five Myths of Cloud Computing](#)

[SOA Centers of Excellence: Preserving Order Amid Change](#)

[Recording and Quality Monitoring for Regulatory Compliance](#)

[7 Email Marketing Refreshes](#)

[Making Shopping Social: Lessons from Ticketmaster](#)

[Seven Qualities of Wildly Desirable Software: Forrester Report](#)

[Endpoint Security - Data Protection for IT, Freedom for Laptop Users](#)

[Innovate the Steve Jobs Way](#)

[ITCAM for Microsoft Applications Customer Implementation Review Case Study](#)

[Best Practices and Applications of TLS/SSL](#)

[More whitepapers »](#)

## Featured Whitepapers

VeriSign  
Authentication Services



### Best Practices and Applications of TLS/SSL

TLS (Transport Layer Security), widely known as SSL (Secure Sockets Layer), is the most well known method to secure your web site. But it can also be used for much more.

## Whitepaper Alerts

Get updates on white papers, case studies, and spotlights on tech products and solutions for your business.

Enter e-mail address

## More from the PCWorld BusinessCenter



[How Adobe Flash Lost Its Way](#)



[Amazon Kindle Fire First Impressions: Solid but Limited](#)



[Amazon's Kindle Fire Tablet vs. the Competition: Spec Showdown](#)



[About Us](#)  
[Contact Us](#)  
[FAQ](#)  
[Magazine Customer Service](#)

## Resources

[Twitter](#)  
[RSS](#)  
[Newletters](#)  
[Advertise](#)  
[Ad Choices](#)

## Network

[PCWorld](#)  
[PCWorld Business Center](#)  
[Search for Tech Jobs](#)  
[Careers at IDG](#)  
[Macworld](#)  
[MacUser](#)  
[Mac OS X Hints](#)  
[iPhone Central](#)



Name

City

Address 1

State Zip

Address 2

E-mail (optional)

[Canadian Residents](#) | [Foreign Residents](#) | [Gift Subscriptions](#)  
[Customer Service](#) | [Privacy Policy](#)