THE CONVERSATION

Ashley Madison breach reveals the rise of the moralist hacker

July 21, 2015 3.13pm BST

Bill Buchanan
Head, Centre for Distributed Computing, Networks and Security at Edinburgh Napier University

Tell no one… that we've just lost all your data. ALM

There's value in more than just credit card data, as Avid Life Media (ALM), parent company of the extramarital affair website Ashley Madison, has found out after being raided for millions of their customer's details.

All sorts of information that isn't expressly financial is valuable – HR records including personal information and health information, such as those stolen from the US government, can be used to fraudulently gain access to other data, of for blackmail for financial gain or to further a political or moral agenda.

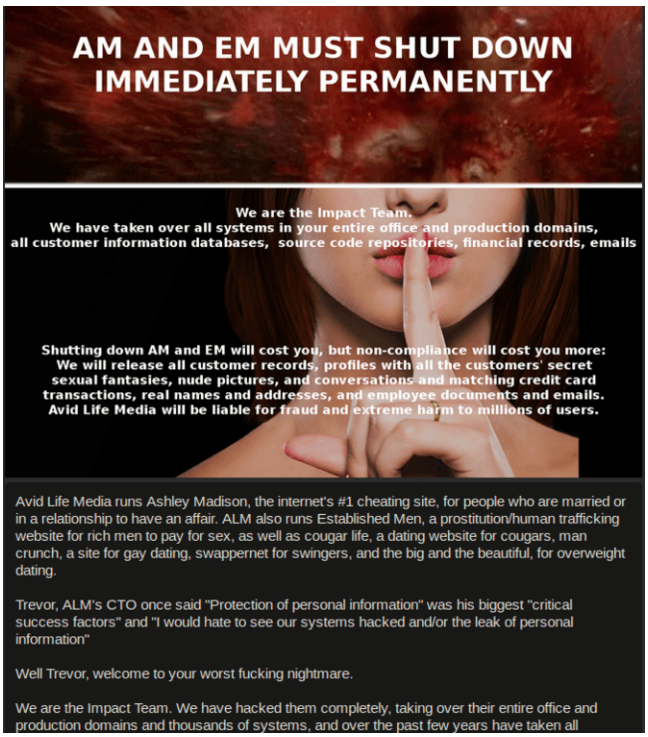
The Ashley Madison hackers, calling themselves Impact Team, seem to have a moral agenda, adding another dimension to the factors that motivate cybercriminals, and therefore something else for overburdened security professionals to consider.

It doesn't get more sensitive than this

There is a spectrum of sensitive information, from an email address to private secrets. The theft of the Ashley Madison databases, essentially a list of 37m possible adulterers' identifying details, must rank as one of the most "sensitive" troves of data ever acquired.

While there will be credit card details too, it's the potential for public (and private) embarrassment that many will be fearing.

Reported by security research Brian Krebs and confirmed by Noel Biderman, CEO of Avid Life Media (ALM), Impact Team's statement rails against the motivations not just of the supposed cheaters using the site, but the site itself for facilitating this behaviour, demanding that ALM close down Ashley Madison and another of its sites, Established Men, permanently or risk the details being published.

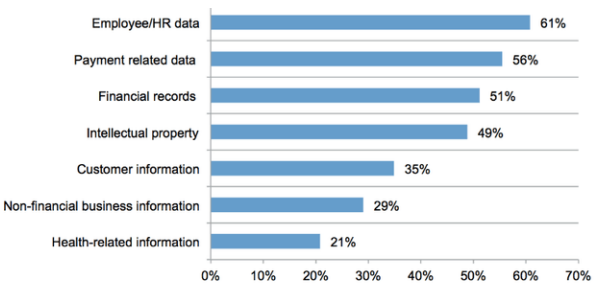


The message left by Impact Team hackers.
ImpactTeam/Krebs on Security

Impact Team's ire is directed particularly at ALM's "full delete" service where, for US$19, all a user's details will be deleted. They claim ALM made US$1.7m from this service, yet leave the credit card details, obviously including real names and addresses, intact. Impact Team hint that the hack was made possible through an insider – embarrassing for a firm that had aimed to raise US$200m this summer from an IPO .

Encrypt! Encrypt! Encrypt!

According to a recent survey by Thales, typically the most sensitive data that is encrypted is employee and HR data. It goes without saying that this is highly sensitive information that can bring repercussions both on the individuals and the firm in question. As customers, we may not be pleased to note that customer details are some way down the list. Really, all these aspects should be closer to 100%.



Regularity with which certain types of company data are encrypted. Thales

Intellectual property is certainly a target for cyberattacks, with the loss of source code and secret product information potentially disastrous for companies. Hacking Team recently found the internal code of their commercial hacking tools posted all over the internet, for example.

When university researchers analysed 300 discarded hard disk drives they found that a third contained personal data including health and banking information (including a €50 billion euro currency exchange service), and even details for a missile defence system. The lack of planning and care in how this information was dealt with is astonishing.

Poking the hornet's nest

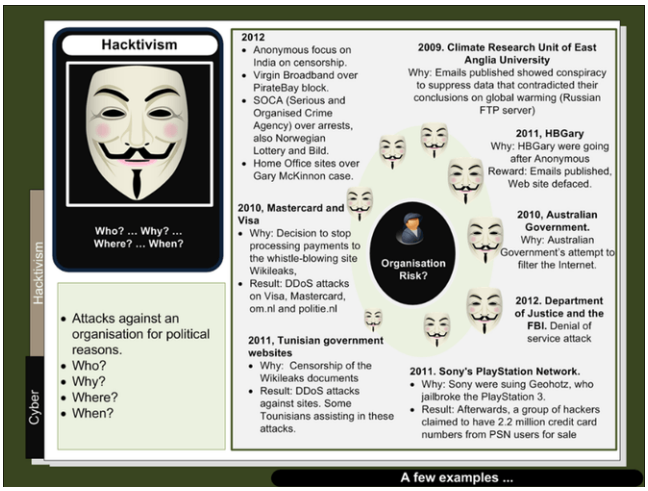
The catastrophic raid on Sony's corporate network last year was blamed on North Korea, but Sony has battled Anonymous, Lulzsec and Lizard Squad over the years, often over their stance on breaches of copyright. Again, a disgruntled insider within Sony is the most likely source of the breach. The hack led to all manner of documents appearing online – such as embarrassing emails from senior executives.

Sony's trouble with hacking organisations can be traced to its court case against George Holtz, who Sony sued after he published root encryption keys for the PlayStation console. Sony demanded identifying details of visitors to his website and social media pages, and was given access to Holtz's PayPal account. The case judge eventually granted Sony permission to view IP addresses of everyone who visited Holtz's site, geohot.com. In April 2011, Sony settled the lawsuit out of court, but have since faced many further attacks.

The rise of moral and political hacktivism

The fact is hackers are increasingly pursuing a variety of agendas. In protest at St Louis County Police involvement in the death of unarmed teenager Michael Brown in Ferguson, Missouri, the police department's website was attacked, knocking it offline for several days. The group responsible declared they had gained access to dispatch tapes related to the day of the shooting, which they then uploaded to YouTube.

In political actions worldwide, from the Arab Spring uprising, to Russia's suspected cyberattacks on Estonian government websites, or the Syrian Electronic Army, the internet is increasingly a new vector of attack. The internet as battleground is not in the future, it is already here, and as attack on the French channel TV5Monde should remind us, it may escalate to include control of news outlets too.



Hacktivism, where cybercriminals can also be freedom fighters. Bill Buchanan, Author provided

Organisations need to understand that there are new risks and new ways to distribute messages, especially from those skillful enough to disrupt traditional methods. It's important to note that the viewpoint of the hacktivist will often be reflected in the political landscape of the time, and that this is subject to change. The hacktivist, a cybercriminal to some, can be a freedom fighter to others.

Be pure in thought and word and deed

The internet provides a voice for all, and there are many examples where corporations, organisations or governments have outraged groups around the world who have successfully staged an uprising or retaliation against them. Someone may be small on the internet, but can still have a massive impact. Sony lost billions of dollars from its share price, and forfeited a great deal of customer confidence.

A strong defence is the starting point, but if there is trusted internal access then it is possible to circumvent the locks. With digital media cards now supporting hundreds of gigabytes of data it's not too difficult to take huge amounts of data off-site – and this is why encryption is so vital. In short:

Encrypt sensitive data
Control and limit access to sensitive data
Make sure those controls work
Check who has access to the data
Integrate multi-factor authentication for the access to sensitive information
Watch where you back up your data and protect that too
Don't use the same encryption keys for everything

And finally, try not to upset people. Ashley Madison rashly boasted of its superior security, while flaunting what many would describe as unethical behaviour. Such things are red rags to a bull. Companies need to understand that their insecurity today is as much to do with their behaviour and the reactions or political and social aims of others in response as it is the straightforward quest for financial gain.