

There have been many column inches dedicated to the PlayStation Network, which was taken offline following a breach. It has been a high profile incident and has left Sony management red-faced with many questions thrown at them – not all of which have been answered convincingly. It is simply not possible to protect against all possible security flaws in a product – but proper risk assessment at least indicates what these might be, and allows an informed decision. This is important for both companies, and for you, the consumer.

You may not be Steve Jobs or Steve Ballmer. The company you work for may not have an online gaming community and you may not sell games consoles, but it is certain that you are the consumer for goods and services that you would at least hope include security as part of what you've bought into. If you put your money in a bank, you hope it's still there when you want to withdraw it. But, more importantly, security is becoming more important as so many products include a technology enabled element. For example, maybe you bank online these days.

So there are many lessons one can draw from the Sony incident, as an individual, from a technical perspective, and from a business perspective. In particular, the incident illustrates the impact of weak risk management culture – perhaps because it was felt that consumers did not think that security was important.

### The PlayStation Network

Sony's PlayStation Network service is a powerful customer proposition. Aside from allowing user to compete in online gaming, browse the Internet stream films, and more. Its prime attraction rests in the ready supply of downloadable games. This attractive and easy-to-use package has over 77 million users around the world – 3 million in the UK alone. But what sits behind this?

**Point 1:** Ease of access to services tends to mean quick authentication and seamless payment, which means that user details, including card details are stored somewhere easily accessible. Where you have such data stored, you have something worth stealing.

**Point 2:** The end user ( the PS3 gamer at home) may think that they bought in to a secure product – after all, they've put in a password – but what they couldn't see was that the infrastructure supporting it was not secure.

**Point 3:** If you're releasing a product for the young and technology literate, which needs to be globally accessible, you're also mapping quite neatly onto the demographic who are often keenest to experiment with breaking technology. Neither of these are particularly arcane facts, so what (may) have gone wrong?



### Sony's story

According to Sony, the incident was an "external intrusion", which certainly resulted in the compromise of certain portions of customer data, including:

- Your user name
- Your address (city, state, and postcode/zip)
- Country
- E-mail address
- Birthday
- PSN password and login name

Additionally, it appears that some further data has been compromised- including credit card details, and the details of subordinate accounts (e.g. where parents held the primary account and also paid for children's ones). Certainly some press reports suggest this has been the case. Sony's advice has been to act with caution – to report to your bank that your card data may have been compromised.

Initial suggestions from Sony that the incident was orchestrated by hacktivist group Anonymous have since been dismissed by the group. Anonymous were quick to issue a denial of this accusation. This seems to have been an attempt by Sony to excuse the incident and is in any case an irrelevance: the root causes of the incident were endemic, not a result of the actions of external influences.

### Security Assessment – How it should work

In theory, there is an accepted set of principles for organisations (for example governments) or businesses which are launching a new technology offering – for example, an online store. This can be summarised as:

- 1) The organisation has it written down in a policy that new products need a security risk assessment
- 2) At an early stage in a new project, they speak to their security experts to tell them what sort of security features they need to build in to the product
- 3) Before the product is launched, testing is done to make sure all the expert's requirements have been met – this might include penetration testing (ethical hacking)
- 4) Any problems that are found are reported and fixed before the product goes out to the market.

The reality is often quite different. If an organisation thinks other things are more important than a secure product, for example, getting to market quickly, it might be skipped over. Often consumers don't ask for security as part of what they're buying – how many teenagers really thought about the risk to their parent's payment details when they said they wanted a PS3? Sometimes the security professionals may come up with findings which are difficult to understand, very complex, or not stated clearly. And sometimes they will be drawn into a project when it is just too late for them to make a big difference.

### Sony's story

The business culture within Sony may be an important factor here – it is not the first time that Sony has played fast-and-loose in this area. In October 2005, it was alleged that Sony's music CDs had installed a rootkit on the user's PC as a Digital Rights Management measure. This was not merely difficult to detect and remove; it also constituted a crime in many countries. Arguably, it posed significant security risk to affected users.

So was it the case that security concerns were simply subordinated to marketing ones? Developers may have been pushed to “deliver” a product with little or no built-in security, either because that is how their task was defined, or because they simply lacked the training. If delivery was time pressured, then there may have been little scope for robust security testing on the supporting infrastructure. After all, the user end was secure – why bother with anything else ?

Yet, there is also another cultural perspective, around organizational decision making. In highly hierarchical organizations, real decision making power tends to be heavily concentrated at the “top” of the organization - a level at which technical experts tend not to be operating, or indeed be very welcome. Risk assessment is not easy – it is even harder if one does not have access to the facts. This tends to lead to senior management “deciding” what the risk is, rather than actually assessing it (which is messy and involves getting into detail).

So did Sony management make such a decision as a matter of policy or around such a flagship product specifically? This would certainly set the scene for what has subsequently unfolded. Were risk assessments conducted properly or are shortcuts taken to skim through the process in order to meet deadlines? Was the network adequately segregated to keep the gaming sections isolated from payment systems? Was there enough time given to allow thorough system testing? Many companies tend to skim on this part by releasing 'beta' code and allowing their customers to report bugs. Whilst this may be convenient and cheap, it's not always the right thing to do.

### Lessons Learned

It would be easy to dismiss the incident as being simply rooted in incompetence. However, this is simplistic and not very helpful. Therefore there is good reason to reflect on some of the major themes coming out of the incident, from the point of view of a company and an individual.



### A company perspective

Once the PlayStation 3 is in the hands of the end user, Sony is virtually powerless over any modifications the user chooses to make. Therefore, any security that is built into the console can be rendered useless. If you deliver a product or piece of code to your customers, how much reliance do you place on that product not being tampered with in any way?

As any criminologist will tell you, for a crime to take place there needs to be opportunity, incentive, and motive. An online portal like the PlayStation network, or website, or a banking application is built to be accessed by the world. It is designed as a way in to something of value. Therefore without a doubt it will be attacked by some people. The question no longer is, will you be attacked - but will you be able to detect, preferably prevent and recover from an attack in a timely manner?

With this last point in mind, it is worth considering the end-to-end security of a product – it's no good if one part is "unbreakable", but the supporting infrastructure is full of security holes, as seems to have been the case with Sony. A hacker doesn't think like a project manager – they will be looking for holes in the fence, not worrying about which project built which bit of it.

Sony took the decision to take the PlayStation network down upon discovering the breach. As an organisation, Sony have a buffer whereby they can afford to take the network down for days, even weeks with manageable revenue loss. But if you're a company only engages with your customers via the internet, can you afford to take your systems offline in the event of a breach? This is particularly true of smaller businesses.

### An individual perspective

Don't become the weak link in the defences. For example, many people will use the same password for more than one system. So the password they use for their PlayStation Network, will most likely be the same password they use for their email, banking, Amazon, Ebay, Paypal etc. What this means is that a breach of password in one system can impact someone in lots of ways – and most of the immediate impact of a problem will fall on you, as it is you who will have to cancel bank cards, and so on. How many parents thought about that when they provided their card details to PSN ?

Think before you share details with a company online - how confident are you that they are protecting them adequately ? Have you asked ? Even if the company has a relatively low-value service or product offering, they have the same obligation to protect your password as does a bank. You are doing everyone a big favour by asking "how secure is your online product?" It shows the company that you are buying from that security is important.

Remember you have legal rights. In many countries, and particularly in the EU, there is legislation around how organisations are allowed to gather, store, process, and secure your personal information. Of course, this doesn't by itself prevent security incidents – no more than having laws stops crime – but it can be a useful reminder to organisations and companies that they should take your concerns seriously.



### The Future

Eventually Sony will recover from the attack. The PlayStation network will be back online and users will occasionally remember those weeks they had to spend without online capability.

As more breaches occur, customers will demand that a key characteristic of your product or service is that it is secure – after all, it is their data which is at risk, and them that have the hassle of cancelling cards, etc. This should be the driver for business decisions around security, not simply the detail of consumer rights under legislation. The media seem to think so too, and are keener now to call out stories around security compromise than ever before.

The motor industry has evolved over the last couple of decades, with more emphasis being placed on car safety. Just how when a motorist is involved in an accident, they have trust that their seatbelts, airbags and other security measures will save them from serious injury or death; companies need to gain their customers trust, that even if something happens, their data will remain safe. Natwest is one of the largest retail banks in the UK, and is part of the RBS Group. A good example of recognition of security as part of the value of a product is the inclusion of security measures in the Natwest Customer Charter. This document is published on a yearly basis, detailing the organisation's performance against a range of measures, and it is supported by TV advertising.

Lastly, consider the long term impact of security failures – if PSN was not secure, as have several other Sony sites, what other Sony products, services, or infrastructure are now being inspected with interest? And what happens when all those 14-year olds come to making their next technology purchasing decision?

