

Sony Breach: Lessons Learned



Some Facts From Ponemon

Median annualized cost of cyber crime for 50 organizations studied was \$5.9 million per year.

- Range: \$1.5 million to \$36.5 million each year.



Some Facts From Ponemon

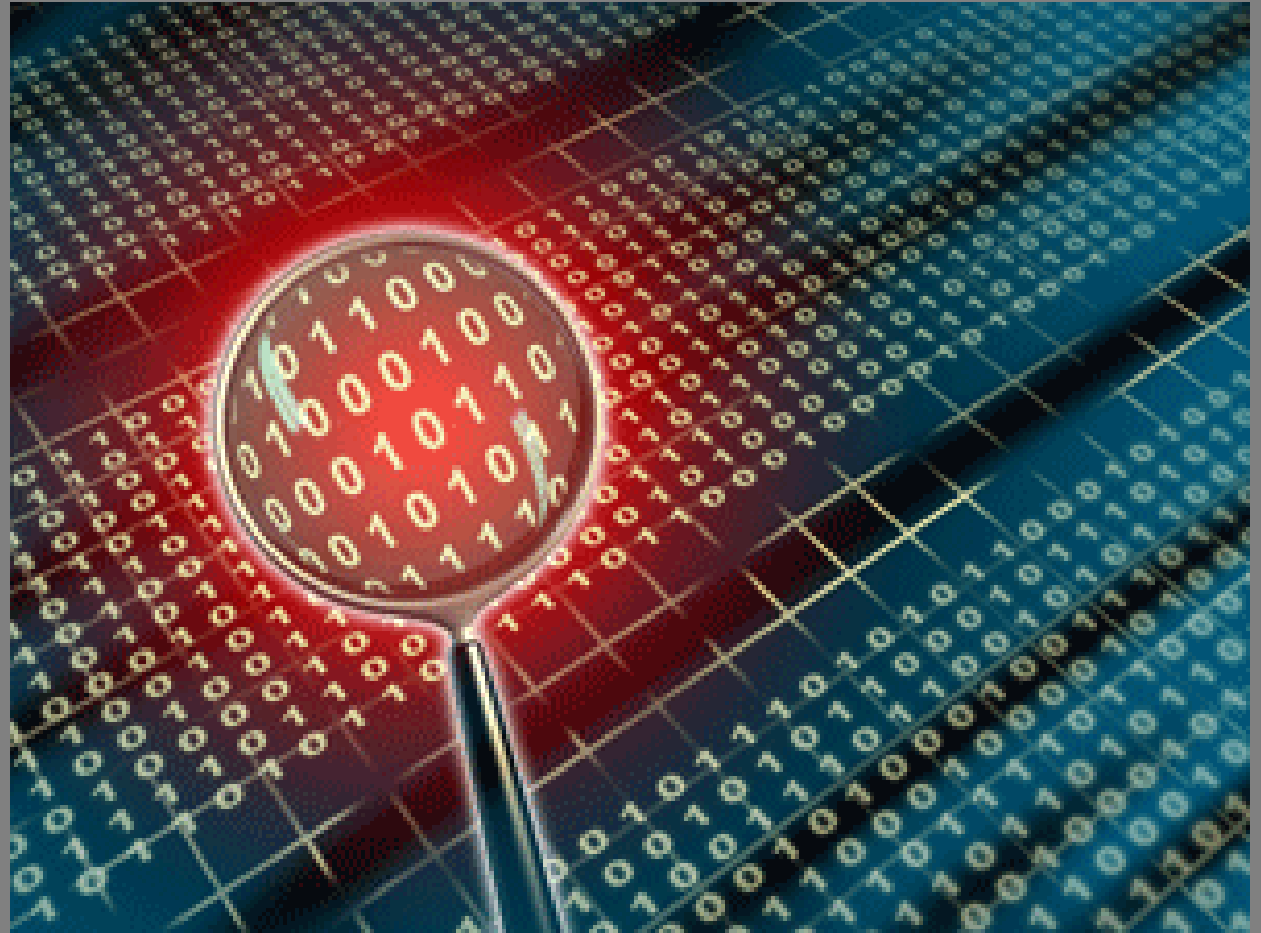
Average of 72 *successful* attacks per week across the 50 companies (more than one per week per company).

- Increase: 44% from last year's successful attack data.



What Kinds of Attacks Were Costliest?

Malicious
Code



What Kinds of Attacks Were Costliest?

Denial of Service



What Kinds of Attacks Were Costliest?

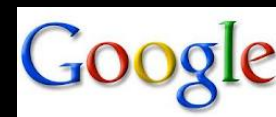
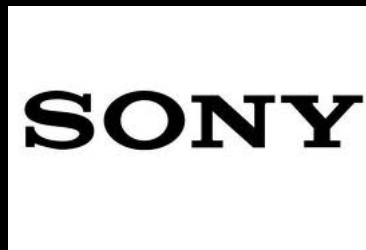
Stolen
Devices



What Kinds of Attacks Were Costliest?

Web-Based
Attacks





Sony Breach Timeline

- January 11 - Sony sues George “GeoHot” Hotz and others for jailbreaking, or circumventing the security system of the PlayStation 3.
- January 27 - Sony asks for a temporary restraining order stopping Hotz from further distributing the jailbreak tools to users, who can download them and break the security on their machines so they can run unauthorized software.
- February 12 - Hotz posts a rap video on his YouTube page explaining his side of the case. (It now has 1.8 million views).
- February 19 - Hotz starts a blog about the lawsuit.
- March 6 - Court approves Sony request to access all the internet protocol addresses of the people who visited GeoHot’s blog to download the jailbreaking tools.



Sony Breach Timeline

- March 23 - Sony claims that Hotz has fled to South America and destroyed evidence. Hotz's attorney denies it.
- April 3 - Hacktivist group Anonymous launches a cyber attack against various Sony web sites in an operation called #OpSony in retaliation for Sony's pursuit of George "GEOHot" Hotz and Graf_Chokolo.
- April 11 - Sony settles the PS 3 jailbreaking case with Hotz. Anonymous says it will continue with boycott of Sony on April 16.



Sony Breach Timeline

- April 19 - 4:15 pm Pacific time. Members of the Sony Computer Entertainment network team detect unauthorized activity in the PlayStation Network system in San Diego, Calif. Certain systems are rebooting when they are not scheduled to do so. The network service team starts reviewing the logs from the system to see what is wrong. It takes four servers offline.
- April 20 - early afternoon. Sony's team discovers evidence that an unauthorized intrusion has occurred and that data of some kind has been transferred off the PSN servers without authorization. Six more servers are found to have been possibly compromised. Sony hires a forensic investigation team that afternoon. That team begins to "mirror" Sony's systems, a meticulous process.



Sony Breach Timeline

- The team can't determine what has been taken and so it shuts the network system down. At that point, the 77 million registered users of the network can't play online games, access their accounts, or purchase movies and other entertainment on the network. Sony's experts have to delve through 130 servers and 50 programs.
- April 21, 2011 - Sony hires a second computer security and forensic consulting firm to provide more manpower.



Sony Breach Timeline

- April 22 - The forensics team completes the mirroring of nine of ten servers that are believed to be compromised. Sony Computer Entertainment's general counsel provided the FBI with information about the intrusion. Sony's forensics team has not reached any conclusions at this point.
- April 23 - Sony's forensics teams confirm that very sophisticated and aggressive techniques were used to obtain access, hide their presence from system administrators, and steadily escalate their privileges inside the servers. The intruders deleted log files to hide their work. Sony now realizes it needs yet another forensic team to help.



Sony Breach Timeline

- April 25 - The forensics teams determine the scope of the personal data that has been stolen from all PSN and Qriocity service accounts, but the team does not know if credit card numbers have been accessed.
- April 26 - Sony provides public notice about the intrusion. It also notifies regulatory authorities in a variety of states about the criminal intrusion.
 - The PlayStation network has been down for 6 days.



Sony Breach Timeline

- April 29 - House of Representatives subcommittee asks for more information on the attack as it considers legislation to require companies to notify consumers in case of data theft.
- April 30 - Sony's No. 2 executive, Kazuo Hirai, apologizes to Sony's customers and holds the first public press conference about the attack. He says the PSN should be up within a week and that Sony has beefed up its security.



Sony Breach Timeline

- May 1, 2011. Sony finds new evidence that hackers broke into the servers of Sony Online Entertainment, the PC online gaming division of the company which runs online games such as Free Realms and EverQuest. Sony discovers a file that says “Anonymous,” “We are legion.” That’s the slogan for the hacktivist group.
- May 2, 2011. Sony says it will explain what happened to Congress but won’t testify yet.
- May 4, 2011. Sony sends letter to Congress answering questions.



Sony Breach Timeline

- May 5 – NY attorney general subpoenas Sony and the same day the CEO offers the first apology and explanation for what may have happened
- May 6 – According to reports, a security expert testifies to a House subcommittee that Sony knew it was in possession of outdated security software
- May 7 – Sony says the PlayStation network might not be up and running as quickly as they thought due to more testing needed
- May 12 – Sony announces “perks” post-breach



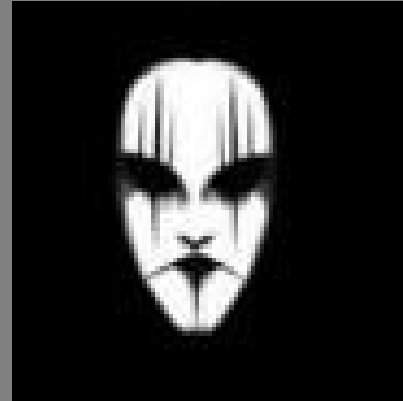
Sony Breach Timeline

- May 14 – Sony begins relaunch of PlayStation Network in stages
- May 16 – Japan's government announces they are waiting for better security measures from Sony
- May 23 – Sony Music Japan. The Hacker News reports that Lulz Security used another SQL Injection method on www.sonymusic.co.jp to reveal database structure.
- May 25 – Sony discloses compromise of 8,500 Greek user accounts and its sites hit in Thailand and Indonesia.



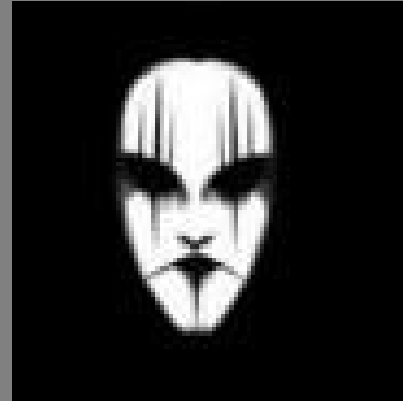
Sony Breach Timeline

- May 27 – Sony Ericson (Canada). Sony discloses shut down and data loss from Sony Ericsson's Canada website; data for 2,000 people, including names, email addresses and encrypted password, appear on The Hacker News web site. The Hacker News attributes the attack to Lebanese Hacker "Idahc_hacker."
- June 2 – Sony Pictures. LulzSec makes clear that they are behind the recent breaches, boasting of acquiring more than 1,000,000 user passwords, email addresses, home addresses, dates of birth, and administrator passwords.



Sony Breach Timeline

- June 3 – Sony Europe. Idahc uses another simple SQL injection method to gain access to 120 usernames and passwords in plain text, mobile phone numbers, work emails and website addresses.
- June 5 – Sony Pictures Russia. Unknown hacker uses another simple SQL Injection method to gain unauthorized access. The extent of the breach is still undetermined.



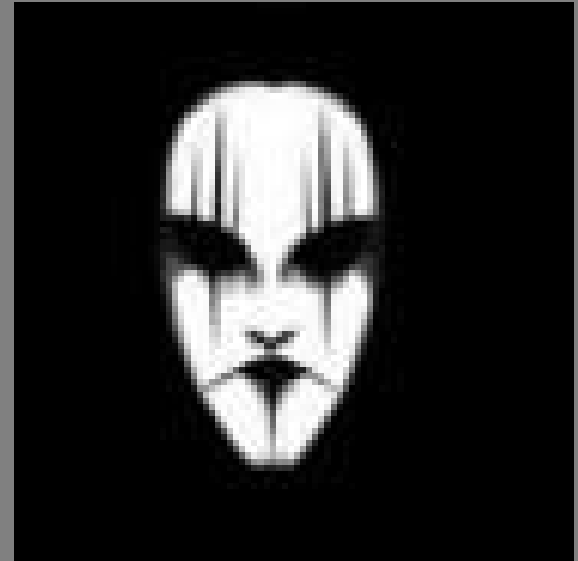
Sony Breach Timeline

- June 6 – Sony CED Network. In a couple of tweets LulzSec presented Sony Computer Entertainment Development Network source code out into the wild. SQL Injection method to gain unauthorized access to 120 usernames, passwords (plain text), mobile phone numbers, work emails and website addresses.
- Via mediafire.com they shared the source code in a 58MB download in the form of a torrent. The torrent also publicized Sony BMG internal network diagrams, including details of hub sites, router IDs, Circuit IDs, IP addresses, site contact names and phone numbers, VLAN information, networking product make, model hostname and management IP addresses.

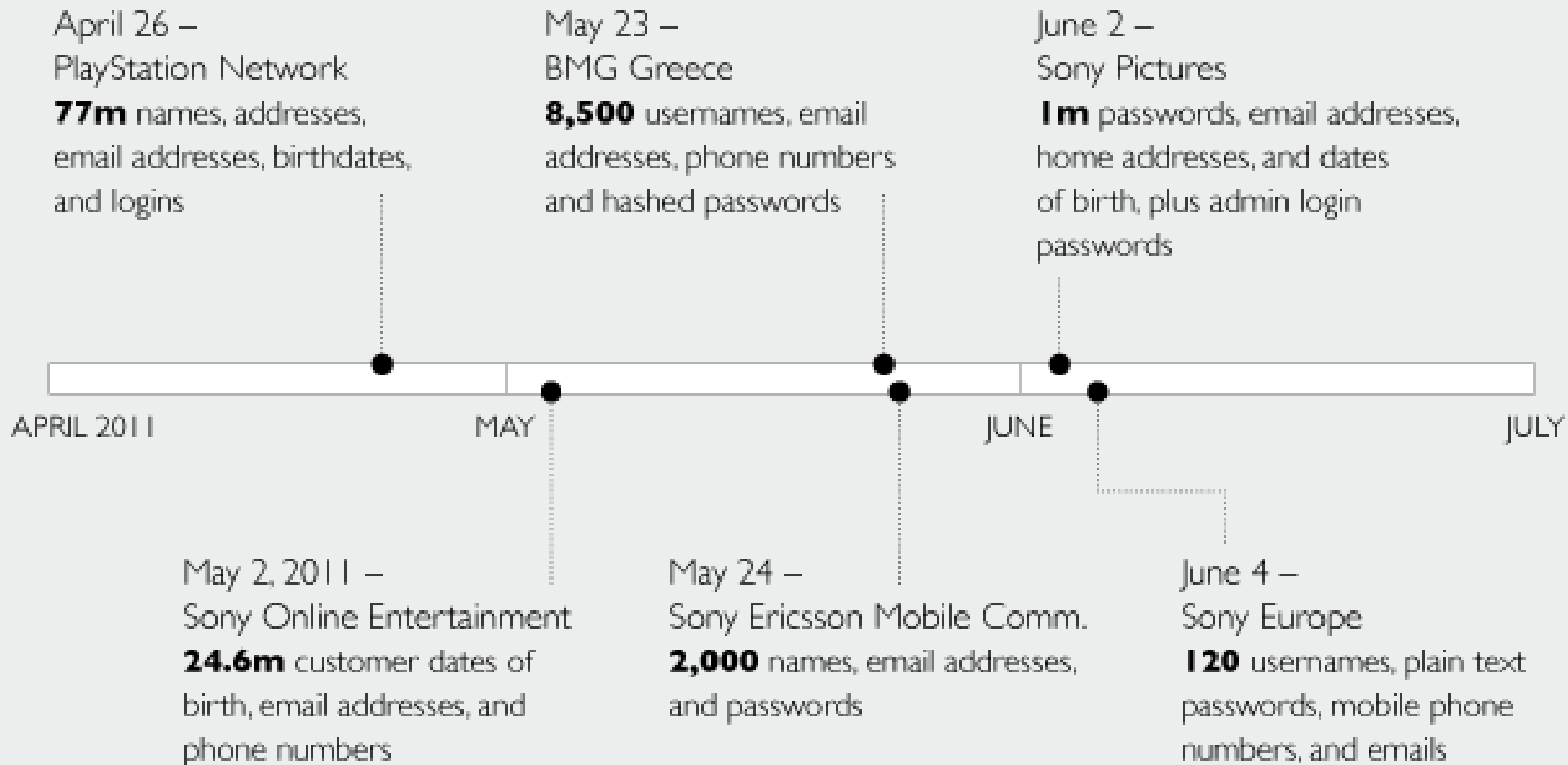


Sony Breach Timeline

- June 8– Sony BMG Music Portugal. Idahc declares that he is a "grey hat" hacker, and backs up his statement by only dumping Sony customers' email addresses, and not the entire database.
- June 19 – Idahc and Auth3ntiq team up to hack Sony Pictures France. They again declare that they are not black hatters.



SONY DATA BREACHES – 2011



Lesson 1: Breach is Inevitable



Lesson 2:

**KNOW YOUR
ENEMY**

The text 'KNOW YOUR ENEMY' is presented in a bold, blocky font. The top row, 'KNOW YOUR', is rendered in a dark red color with a distressed, splattered texture. The bottom row, 'ENEMY', is in black with a similar distressed texture. The background is white, featuring several red and black ink splatters and dots scattered around the text, particularly above and to the right.

Today, Hackers Come in ?



Just Building a Thicker Wall Is No Longer Sufficient

- Intrusions are multi-faceted, and sometimes without singular purpose.
- Advanced Persistent Threat (APT). Walls and alarms are not very effective, and the threat presented by an APT attack is significant.
- Ponemon reports that "The cost of cyber crime is moderated by the use of SIEM [Security Information and Event Management] SIEM companies experienced substantially lower costs of recovery, detection and containment than non-SIEM companies." The cost difference was about 24%. SIEM companies were more likely to recognize the existence of APTs.



Lesson 3: Review Insurance Policies to Ensure Proper Coverage



- Soon after Sony announced the breach, Zurich sought a declaration that it has no duty to defend or indemnify Sony against customer class actions and related matters.
- Zurich sold primary commercial general liability (CGL) and excess liability policies to Sony.
 - Zurich claims that the lawsuits arising out of the cyber attacks are not covered by the "bodily injury," "property damage" and "personal and advertising injury" coverages provided by its liability policies.
 - Zurich also claims that the lawsuits against Sony are excluded by its policies.

IRONY?

theguardian

[News](#) | [World](#) | [Sports](#) | [Comment](#) | [Culture](#) | [Business](#) | [Environment](#)

[Money](#) [Insurance](#)

Zurich Insurance fined £2m for losing customer details

Fine is largest apportioned to one firm by Financial Services Authority, after loss of 46,000 customers' details in 2008

Jill Insley

guardian.co.uk, Tuesday 24 August 2010 07.12 EDT

IRONY?

“

Margaret Cole, the FSA's director of enforcement and financial crime, commented:

"Zurich UK let its customers down badly. It failed to oversee the outsourcing arrangement effectively and did not have full control over the data being processed by Zurich SA. To make matters worse, Zurich UK was oblivious to the data loss incident until a year later.

"Firms across the financial sector would do well to look at the details of this case and learn from the mistakes that Zurich UK made."

Lesson 4: Transparency May Be Your Only Option

- Sony acted understandably in delaying any announcement.
- The law did not require notice before they understood what had happened.
- Yet – Six days was too long. The public and regulatory officials demanded answers with little forgiveness.



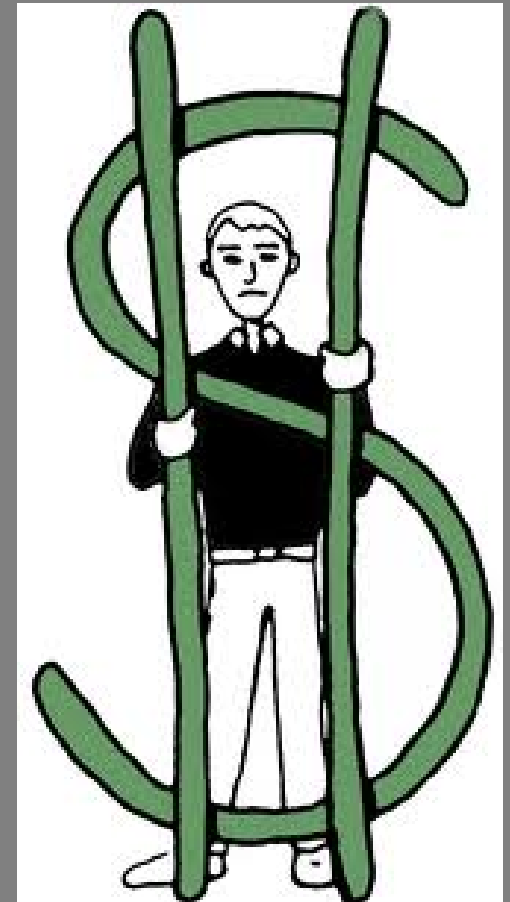
Lesson 5: Merchant Agreements with Credit Card Issuers Can Have Short Fuses

- Each merchant agreement specifies different response deadlines for notice once loss of credit card information is confirmed. Some of them are as short as 24-hours.
- If you fail to meet these deadlines, you may be stuck with all of the bill for remediation.



Lesson 6: Missteps Can Be Costly (but you already knew that, right?!)

- Sony has estimated the cost of remediation at \$171 million (\$2.22 per record).
- But, if the Ponemon Study is right, and the breach costs closer to the average (\$268 per record), then Sony will pay closer to \$20.6 billion.
- Consider the costs of class actions, FTC inquiries, AG actions, and international actions



Lesson 7: Develop an Incident Response Plan Now



- Ponemon estimates that those who do not rush their response pay less. This is likely because they have prepared for a measured, not frantic, response.
- List the things you need to do in the first 72 hours
 - Designate staff with roles
 - Designate how the remediation steps will be documented
 - Arrange an escalation plan and practice it beforehand.

A Few Stories From the Trenches

- Stolen servers from music equipment manufacturer.
 - Unexpected scope of data loss
 - HR and Payroll data
 - Customer data
- Hotel guest billing receipts found in another hotel's business center and a theft from their records room.
 - Credit card merchant agreement deadlines drove the costs of response. The company spent more than it had planned because of the need to compress the response in time.
- Website login credentials.
 - Despite massive number of compromised credentials, the only notice trigger was in Georgia, where the statute covers the lost of usernames and passwords.
 - Password reset and notice did the trick.

Questions?

Joe Cutler
jcutler@perkinscoie.com
206-359-6104