



DIGITAL DISRUPTION WHEN YOU LEAST EXPECT (OR WANT) IT

Craig Pitts

*Global Information Security Solutions
Architect Lead*

Mondelez International

June 2015

TECHLAW AUSTRALIA 2015

Who? What? Where?

- Craig Pitts
 - Career IT, IT Business & Technology, IT Risk, IT Security & Architecture through all sectors
 - Becoming more and more CxO critical advisor, IT Law, Privacy, Legislation, Governance, Board member
- State, National, Regional and Global Management for 15+yrs
- Working for Mondelez, CSC, GE, Novell, HP
- and with global audit firms (PWC, EY, Deloitte)

- Can't be that hard? It's just chocolate and snacks right?
- Well, secrets are secrets and abiding by standards is a mandatory requirement subject to local government laws.
- No-one is above the law and our most stringent critics are our customers. The direct impact is on the bottom line!
- If external IT factors stop, damage or influence our ability to meet all required production and legal requirements, the costs can be huge!

- Australian Privacy?
 - Internet filter?
 - Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015
 - Implements recommendations of the Parliamentary *Joint Committee on Intelligence and Security's* (PJCIS)
- India's Privacy and Data Legislation?
- Malaysia's Privacy and Data Legislation?
- Cross border, Export and Jurisdiction consideration
- Financial obligations (Sarbanes Oxley)



RE: Notice of Unauthorized Use of Paramount Pictures Corporation Property

Dear Sir or Madam:

Irdeto USA, Inc. (hereinafter referred to as "Irdeto") swears under penalty of perjury that Paramount Pictures Corporation ("Paramount") has authorized Irdeto to act as its non-exclusive agent for copyright infringement notification. Irdeto's search of the protocol listed below has detected infringements of Paramount's copyright interests on your IP addresses as detailed in the below report.

Irdeto has reasonable good faith belief that use of the material in the manner complained of in the below report is not authorized by Paramount, its agents, or the law. The information provided herein is accurate to the best of our knowledge. Therefore, this letter is an official notification to effect removal of the detected infringement listed in the below report. The below documentation specifies the exact location of the infringement.

We hereby request that you immediately remove or block access to the infringing material, as specified in the copyright laws, and insure the user refrains from using or sharing with others unauthorized Paramount materials in the future (see, 17 U.S.C. 512).

Further, we believe that the entire Internet community benefits when these matters are resolved cooperatively. We urge you to take immediate action to stop this infringing activity and inform us of the results of your actions. We appreciate your efforts toward this common goal.

Please send us a prompt response indicating the actions you have taken to resolve this matter, making sure to reference the Notice ID number above in your response.

If you do not wish to reply by email, please use our Web Interface by clicking on the following link: <http://webreply.copyright-compliance.com/WebReply?webreplyhash>

Nothing in this letter shall serve as a waiver of any rights or remedies of Paramount with respect to the alleged infringement, all of which are expressly reserved. Should you need to contact me, I may be reached at the below address.

Regards,

- Secret herbs and spices, Freddo, Cola drinks, Oreo cream
- How about:
 - Production equipment recipes, product usage and wastage rates?
 - Critical consumption details
 - Remote modification of actual production runs?
- State sponsored attacks on core and essential services is happening from both East and Western sources (Iranian nuclear centrifuges, American power grids, Indonesia and India)
- Highest bidder wins and takes the data!
 - Russian Mafia make more money through cyber crime and cyber warfare than they do using traditional methods

After email blunder, Woolworths cancels \$1M worth of gift cards

scmagazine.com - 9 days ago

June 01, 2015 After email blunder, Woolworths cancels \$1M worth of gift cards

Australian supermarket chain Woolworths canceled and re-issued more than \$1.3 million (AU) worth of e-gift cards, following an email blunder that revealed the details of thousands of customers and exposed codes for nearly 8,000 shopping vouchers.

On Sunday, Woolworths told [Mashable Australia](#) in a statement that on Saturday, the company was “alerted to a technical fault with an e-gift card offered to customers.”

Fairfax Media, which [initially reported](#) on the incident, obtained a copy of the Woolworths email that was mistakenly sent out. After purchasing gift cards via Groupon, customers were supposed to receive an email from Woolworths containing their voucher information, but instead, a PDF attachment was sent, which linked to thousands of voucher codes.

The email, which also reportedly contained the names and email addresses of customers, was delivered erroneously to more than 1,000 individuals...(continued)



More than 30,000 iiNet customer passwords hacked

June 9, 2015

5 reading now Comments 6



seems westnet, one of aussies biggest ISP's has been owned.



RETWEETS 37 FAVORITES 17



After email blunder, Woolworths cancels \$1M worth of gift cards

scmagazine.com - 9 days ago

June 01, 2015 After email blunder, Woolworths cancels \$1M worth of gift cards

Australian supermarket chain Woolworths canceled and re-issued more than \$1.3 million (AU) worth of e-gift cards, following an email blunder that revealed the details of thousands of customers and exposed codes for nearly 8,000 shopping vouchers.

On Sunday, Woolworths told [Mashable Australia](#) in a statement that on Saturday, the company was "alerted to a technical fault with an e-gift card offered to customers."

Fairfax Media, which [initially reported](#) on the incident, obtained a copy of the Woolworths email that was mistakenly sent out. After purchasing gift cards via Groupon, customers were supposed to receive an email from Woolworths containing their voucher information, but instead, a PDF attachment was sent, which linked to thousands of voucher codes.

The email, which also reportedly contained the names and email addresses of customers, was delivered erroneously to more than 1,000 individuals...(continued)



After email blunder, Woolworths cancels \$1M worth of gift cards

How A Hacker Could Hijack A Plane From Their Seat

May 21, 2015 | by Yijun Yu and Andrew Smith



photo credit: In-flight hacking. Shutterstock

Reports that a cybersecurity expert [successfully hacked](#) into an aeroplane's control system from a passenger seat raises many worrying questions for the airline industry.

It was once believed that the cockpit network that allows the pilot to control the plane was fully insulated and separate from the passenger network, but a flight attendant

s cancels \$1M worth of

celed and re-issued cards, following an email of customers and hers.

lia in a statement that technical fault with an



incident, obtained a copy of the Woolworths email that cards via Groupon, customers were supposed to receive other information, but instead, a PDF attachment was les.

; names and email addresses of customers, was delivered continued)

More than 30,000 iiNet hacked

June 9, 2015

seems westnet, one ISP's has been own



RETWEETS 37 FAVORITES 17



- So we now have easy methods of access (the lesser watched business back doors)
- We have motivated actors (well, we've always had those!)
- We now have a new method! An invisible, well hidden one.
- The techniques are the same though
- Source your crowds to distract (through distributed attacks from drone computers)
- Enable the noise through social mediums such as YouTube announcements (a-la Anonymous)
- Execute while people are distracted with other activity

- It's crime, just not as we know it.





OpenSesame

OpenSesame is a device that can wirelessly open virtually any fixed-code garage door in seconds: **new attack** I've discovered on wireless fixed-pin devices. Using a child's toy from Mattel.

Follow me on [Twitter](#) or [join my mailing list](#) to hear about future projects and research.

By [@SamyKamkar](#)

Live demonstration and full details available in the [video](#):

OpenSesame - hacking garages in seconds using a Mattel toy





OpenSesame

OpenSesame is a device that can wirelessly open virtually any fixed-code garage door in second: **new attack** I've discovered on wireless fixed-pin devices. Using a child's toy from Mattel.

Follow me on [Twitter](#) or [join my mailing list](#) to hear about future projects and research.

By @SamyKamkar

Live demonstration and full details available in the [video](#):

OpenSesame - hacking garages in seconds using a Mattel toy



Image: Dan Hixson/Univers

New tiny silicon chip paves the way for light-speed computers

That means computers and smartphones that run millions of times faster.

BEC CREW 19 MAY 2015



Image: Dan Hixson/Univers

New tiny silicon chip paves the way for light-speed computers

That means computers and smartphones that run millions of times faster.

BEC CREW 19 MAY 2015

Sony Pictures: The Data Breach And How The Criminals Won

+ Comment Now

There are times when I'm simply gobsmacked at the nonsense that transpires in the course of a day. Today sadly, fear uncertainty and doubt won the day over common sense. There has been a lot of press generated about the [Sony](#) Pictures breach. Make no mistake about it, this is as bad as I've ever seen publicly. Let's start off with what we know, Sony Pictures had their digital pants yanked down around their ankles. Like I've said before, I really feel bad for the IT staff that have to recover from this fiasco. What we don't **actually** know is, who was behind this attack. There has been plenty of rumour and conjecture but, lets face it, no hard evidence. Call me old fashioned but, I would love to see some facts.

One fact that has is unavoidable is that the Seth Rogen / James Franco movie, "The Interview" will not be available in theatres to watch on December 25th. Why? Well, an *anonymous individual* posted a threat on the site, Pastebin.com. That post has

OpenSesame

OpenSesame is a device that can wirelessly open virtually any fixed-code garage door. **new attack** I've discovered on wireless fixed-pin devices. Using a child's toy from Me

Follow me on [Twitter](#) or [join my mailing list](#) to hear about future projects and re

By @SamyKamkar

Live demonstration and full details available in the [video](#):

OpenSesame - hacking garages in seconds using a Mattel toy

Open
Sesame
hacking
garages
in seconds



- So we'll move it to the cloud! That's SAFE..... Right?
- It's all in the legal T&C's. This stuff is pure contractual agreements and you will find that the hosted service provider offers very little protection in the event of a breach or loss of your data
- Always look for:
 - Encryption of your data
 - Encryption of your identity and passwords
 - Encryption of your connection to their web services (i.e.: HTTPS)
 - Escrow of your data in the event they fold
 - Country of containment (if you have legislative rqts. More common)
- It's just computer system hosting with fancy name

Report: Apple Knew of Security Problems Long Before iCloud Breach



Kate Knibbs

Filed to: SECURITY 9/24/14 5:10pm

4 1



A software developer [is accusing](#) Apple of brushing off a serious iCloud security flaw that he alerted the company to six months before the recent iCloud celebrity nude photo stealing scandal.

Report: Apple Knew of Security Problems Long Before iCloud each

Continued breaches show Dropbox not secure enough for small businesses

Posted by [Hector Salcedo](#) on Jan 13, 2015 8:42:44 AM

[Kate Knibbs](#)

Filed to: SECURITY 9/24/14 5:10pm

4 1



I'm just going to come out and say it: Dropbox on its own is not secure enough for businesses. Bugs and open-doors leave sensitive files open for viewing and who knows what can happen if your classified information falls into the wrong hands. If you're sharing files with coworkers by sharing Dropbox links, cease and desist! You are potentially leaving your files open to the masses.

Apple developer [is accusing](#) Apple of brushing off a serious iCloud security flaw that he l the company to six months before the recent iCloud celebrity nude photo stealing il.

Problem

Dropbox is currently the top dedicated cloud storage provider hitting 200 million users back in November 2013. Unfortunately for business users, Dropbox is also the most targeted cloud service by hackers and thieves. Remember when hackers held [7 million Dropbox passwords](#) ransom? Not

Managing your Data's Risk in a crazy, crazy world

- Well this all sounds a bit much then. ☹️
- Not really, just ensure the basics are under control
- Get the ownership well understood and then manage it!
 - Keep your contracts up to date with local and federal legislation
 - Keep your audit controls aligned to legislative risk areas
 - Understand what jurisdiction your data resides in and consider the local legal requirements in THAT country!
 - Get it in writing!!
- It really is as simple as:
 - Reviewing access regularly (and removing people who don't need it!)
 - Keeping up with Security patches, Anti-Virus and User access controls

Maybe it's not as bad as we all think

- IT Privacy and Legislative requirements must be incorporated into standard Procurement/Legal contracts
- The vast majority of attacks can be avoided by ensuring companies keep their computing environments patched and protected with current Anti-virus software (Actionable and measurable through Contract requirement and Audit controls)
- Ensure Access to data is managed, ensuring terminated or changed role users have access revoked in a timely manner. Manage that identity!! (Actionable and measurable through Contract requirement and Audit controls)