RSA® Conference 2017

Learning Labs

Cyber-Overlord: Nation-State Cyberattack Exercise (LAB4-W04)

Post-conference summary

Stephen McCombie

Bob de la Lande

eon MEDIA

Table of Contents

Introduction

With so many sessions and Labs to choose from, we were very grateful that you elected to attend ours and we truly hope that you not only had fun, but left the room wanting more.

The session scenario was deliberately complex and we know you had very little time to get your heads around it, but that was the purpose of this exercise.

In a real-life breach, with so many internal and external stakeholders all making demands for information, there is a great deal of pressure on individuals and teams across the business to process and deliver that information as quickly and as accurately as possible.

We believe workshops like this must be a critical part of any strategic crisis management plan to ensure weaknesses and strengths are clearly identified.

Regular workshop audits give you a clear view of your crisis capabilities and the specific actions that are essential to prevent or reduce the impact of a crisis on your business and its stakeholders.

While many of you may never experience the “challenge” of speaking directly with the media or Congress, we included media and congressional interviews to give you feel for the style of messaging that is required … and for a little fun.

We thought you all embraced the process with enthusiasm and, once you understood the scenario, began developing and delivering strong messages which, in most cases, hit the mark.

We thoroughly enjoyed working with you and we hope you found the whole experience worthwhile and rewarding.

Lab Summary

Scenario

We believe in making our scenarios as real and current as possible to better ensure everyone is fully engaged. That’s why we go to the trouble of creating realistic news bulletins which we play at specific times to deliberately apply “more pressure” to an already pressured environment.

At this year’s Conference, our scenario involved a suspected nation state cyber-attack which impacted the government and private entities. It was set in a mythical country, Orangeland, and participants were divided into eight groups, each representing key government, regulatory and business organizations.

Synopsis

- Orangeland is a 1st World nation in the South Pacific region to the East of New Zealand.
- Its capital is Orange City and the country has a population of 20 million.
- It is a high-tech economy and has an advanced governmental structure.
- It is a republic with a Presidential Head of State and a Congress of representatives from all over Orangeland.

- Orangeland has good relationships with countries in Western Europe and North America but in recent time its relations with Ruthenia has been poor.
- Ruthenia is an Eastern European major power whose president, Igor Talin, wants to restore Ruthenia to Superpower status.
- In recent weeks, Ruthenian Navy ships have exercised just outside Orangeland Territorial Waters.
- Orangeland, like many nations, is concerned about the growing threat of terrorism and as part of a broad counter- terrorism strategy, has given the FBI extensive powers to access data of citizens and visitors under the control of Orangeland telcos and private corporations.
- Orangeland's largest telco, OrangeTel, which is also the major provider to government for telecommunications services, has worked closely with the FBI to facilitate their data analysis needs.
- The software and IT services company Clockwork Orange has provided systems and support to OrangeTel and has actively assisted in this work with the FBI.

- An election is looming for Orangeland's presidency. The current president, John Gomes, has reached his term limit and his party, the PPO, have nominated former congressional representative for Orangeland's largest city, Orange City, Melinda Hutchinson. She is a party favorite and well connected, her father having served as Orangeland's president in the 1980s. The OUP, the opposition party, has nominated successful business man Brendan McShane and although he has no previous political experience, he has promised to "Drain the Swamp" of Orangeland politics.

- In the PPO nomination process a left-wing candidate, Tom Masters, from a rural southerly part of Orangeland was defeated by Hutchinson.
- Many of Masters' supporters have suggested the nomination process was fixed since Masters seemed to be leading in many of the polls and looked likely to defeat McShane in a general election if he received the nomination.
- The PPO look to be favorites in the election until an email, purportedly from the President's Office to the PPO Nominee for President Melinda Hutchinson, is released by WikiLeaks. It shows that an agreement was in place to support nominee Melinda Hutchinson over Tom Masters, the more left wing candidate within the party. The President reportedly has called Masters unfit to represent the party according to the email. The email goes onto to discuss ways to prevent Masters winning. Many of the Masters' supporters claim the nomination process was fixed and have asked for an investigation.
- It appears the email has come from accounts with OrangeTel. Orangetel begin an investigation and suspect that the compromise may have been caused by some the functionality that they and Clockwork Orange built in their system to facilitate the FBI data analysis work.
- The FBI are brought in to investigate the breach. They identify some systems in a high school in Orange City where the email was leaked but are unable to determine where it went from there as the system was forensically wiped. But these systems have been used before as jump off points for attacks by suspected Ruthenian SSS (State Security Service) hackers against some of Ruthenia's East European neighbors and their sympathizers in other parts of the world. They also identify the source of some of the traffic to the high school via traffic analysis. The source is a Tor node used in the past by the SSS but also by other hacker groups.
- OIA, the regulator for the Internet, has had a huge number of complaints from users of Orangetel that they may have been compromised and they initiate an investigation.
- The Cybersecurity Congressional Committee for Orangeland, chaired by a member of the OUP, has started an investigation and conducts hearings into the breach and the activities of the FBI data gathering program
- Media interest is growing and putting pressure on all eight government and private organizations and business (the eight table groups). How do they respond??

Exercise Play

All the groups actively engaged in the exercise. We had plenty of interaction between the entities including a joint investigation into the breach by the FBI and the regulator OIA. The political dimension was played out by both political parties and the President's office. Orangetel and Clockwork Orange worked with authorities on the investigation of the breach. CERTOL distributed technical advisories to infrastructure providers. All groups issued media briefings which were of a high standard despite the limited time to fully understand the exercise "world" and the evolving cyber incident.

Comments on Crisis Management

Effective Crisis Management

Effective crisis management does not happen by chance.

Regular planning and workshop rehearsal enables your business, or organization, to better respond in a professional and timely manner which mitigates the crisis impact and allows you to get back to business faster and significantly lessens the impact on your brand and bottom-line.

Workshopping identifies the gaps in your communication plan, effectively prepares key staff for unexpected events and enables your business to recover more rapidly from a crisis.

Planning for the worst is essential in any effective crisis management strategy simply because under-estimating it can have disastrous consequences on brand and reputation.

The difference between success and failure in managing a crisis can often hinge on the effectiveness of the crisis team … effective communication across the team and with key people in the business is essential. That’s why our workshops focus on teamwork and communication.

Feeding the Media

When the media come knocking, speed is crucial. A well-prepared crisis management team will be able to respond immediately, even if it’s only a brief holding statement confirming that the business is aware and looking into it.

Get on the front foot. Fast, effective communication gives you control of the developing situation – this avoids looking reactive or defensive.

If the issue appears to impact stakeholders, always show a human face. Show that you care and are prepared to take responsibility for the situation (which is different from admitting liability)!

Your spokesperson, a well-trained member of your crisis management team, should be personable, well-spoken, and be the confident representative of your business.

Media trained, this spokesperson understands what the media wants and will stick to prepared key messages designed to respond to the issue while demonstrating the organization’s preparedness to be open and sincere.

Further Information

If you would like further information regarding this Learning Lab, running cyber exercises or crisis communications please contact eonmedia@bigpond.com.

Your Facilitators

Dr. Stephen McCombie

Managing Principal, SecureWorks Inc.

As a Managing Principal for SecureWorks, Stephen provides security consulting services to SecureWorks' customers in the Asia Pacific region. Stephen is also an Honorary Research Associate at Macquarie University in Australia and an Honorary Research Fellow at Massey University in New Zealand. McCombie possesses more than 30 years of industry, academic and government security experience including specialized skills in digital forensics, incident response, SOC management and strategic threat assessments. McCombie holds a Ph.D. in computer science, a Master's of IT and a B.A. in international relations. He holds the CISSP, ISSMP and CFE certifications.

Bob de la Lande

Managing Director, EON Media Pty Ltd.

After two decades in print and international broadcast journalism, Bob de la Lande founded EON Media in 1993 believing local and global companies needed a better way to manage their crisis communications and threats to brand reputation. He has provided counsel to senior Ministers in the Australian and New South Wales State governments and delivered strategic communications and media management strategy to many leading Australian corporations and businesses. He has a strong reputation for delivering effective advice in times of crisis, specializing in first response strategies designed to meet media demands and mitigate threats to brand and reputation. De la Lande has anchored several major events, including the 2014 Global Ports Conference hosted by the International Association of Ports and Harbors.

RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: **LAB4-W04**

Cyber-Overlord: Nation-State Cyberattack Exercise

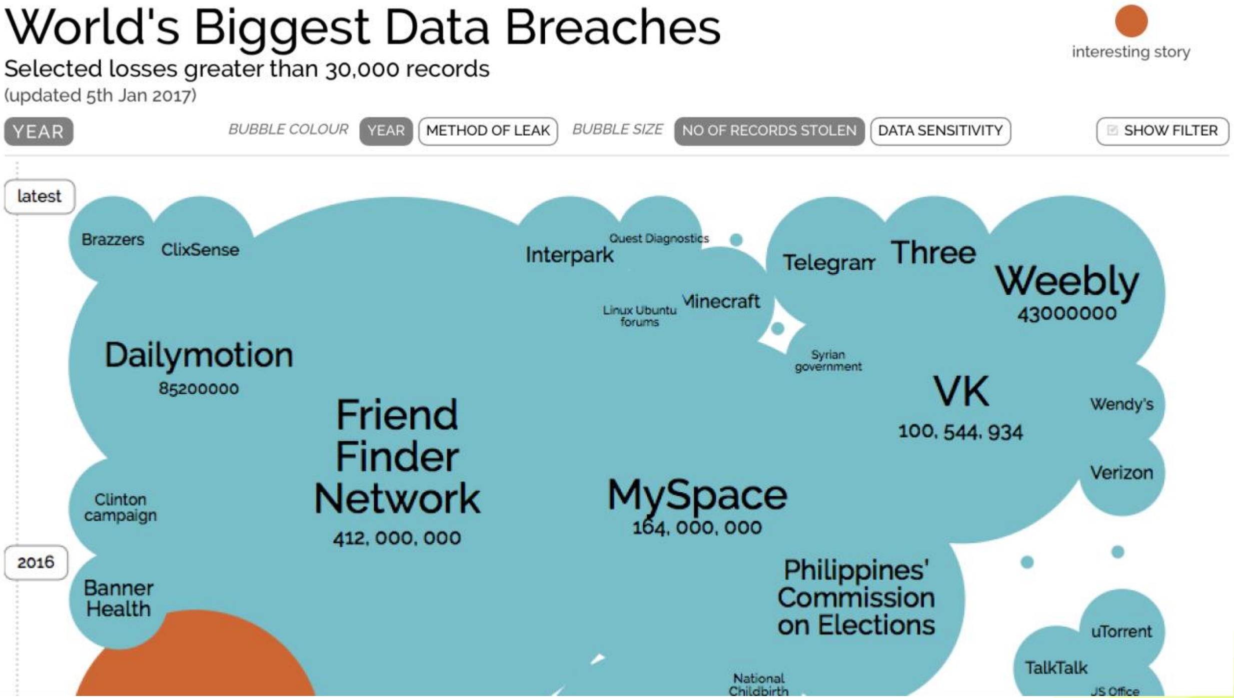
Dr. Stephen McCombie
Cybersecurity Researcher & Lecturer
Macquarie University
Australia

Bob de la Lande
Managing Director
EON Media Pty Ltd.
Australia

Agenda

10:30am – 10:50pm	• Introduction
10:50am – 11:10am	• Incident Scenario
11:10pm – 11:50pm	• Exercise Free Play
11:50am – 12:05pm	• Media Conference
12:05pm – 12:20pm	• Congressional Hearing
12:20pm – 12:30pm	• Exercise Wash-up

Data Breaches Continue Unabated



World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 5th Jan 2017)

YEAR

BUBBLE COLOUR: YEAR | METHOD OF LEAK

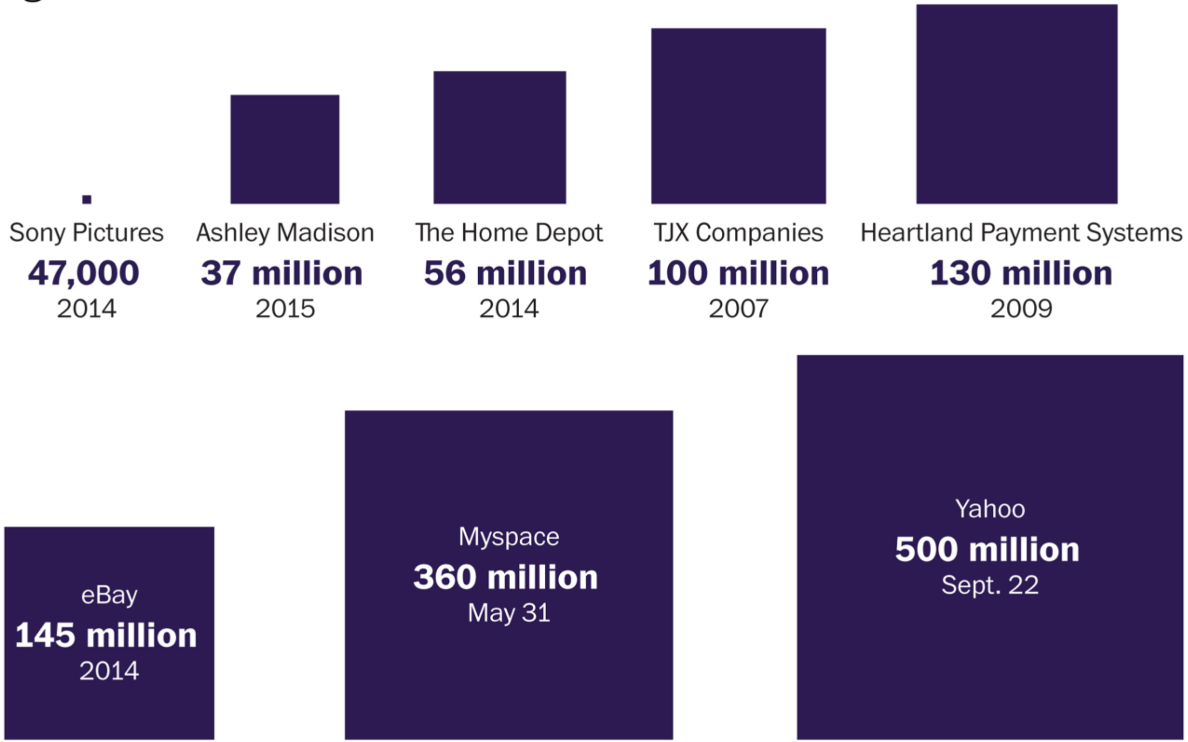
BUBBLE SIZE: NO OF RECORDS STOLEN | DATA SENSITIVITY

SHOW FILTER

● interesting story

Scaling previous data breaches

Yahoo’s data breach affected about 500 million accounts, making it the largest breach on record.

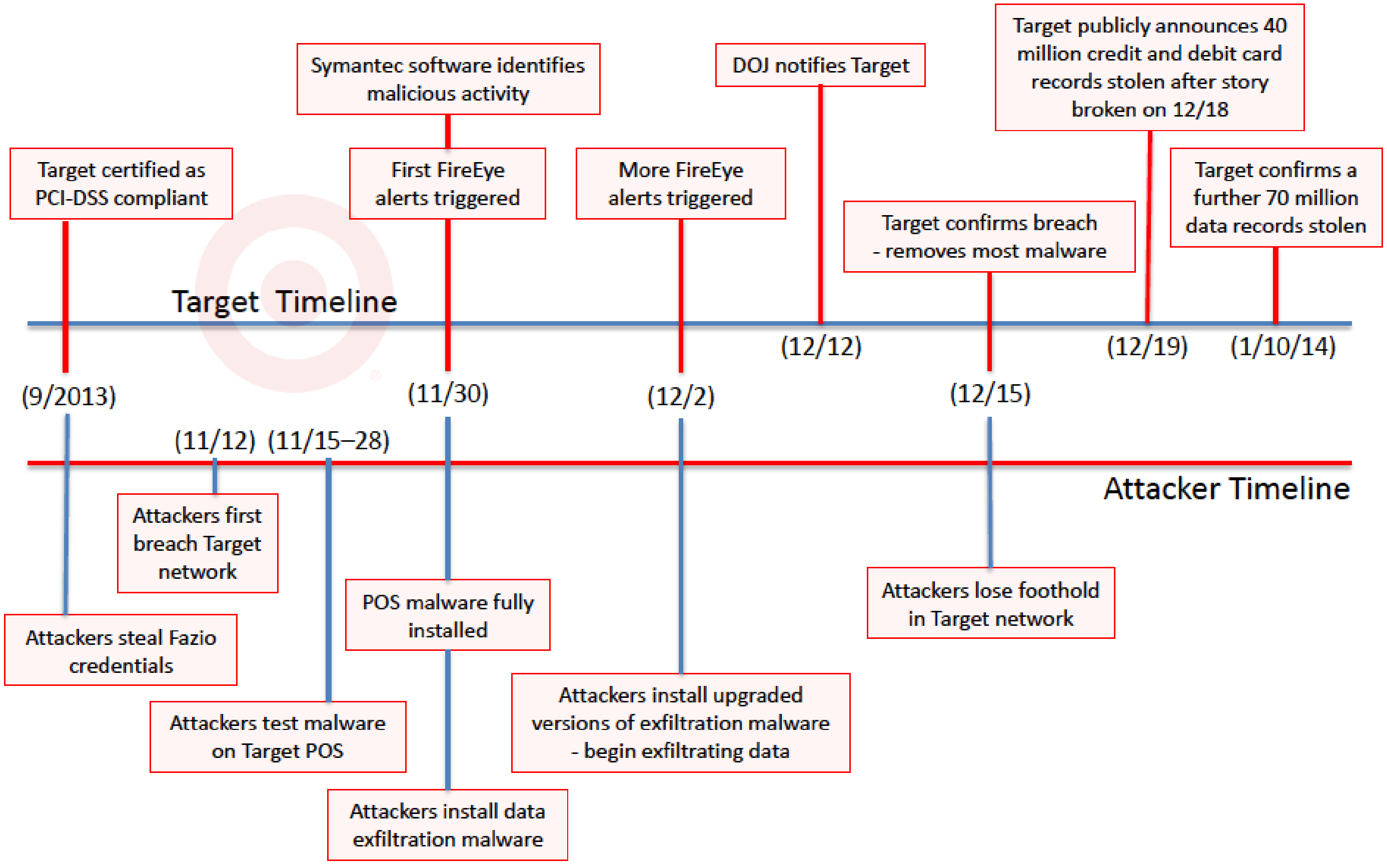


Note: Dates are when officials confirmed a data breach occurred.

Sources: Privacy Rights Clearinghouse, news reports

CHRIS ALCANTARA/THE WASHINGTON POST

A Timeline of the Target Data Breach



Target Timeline

Target certified as PCI-DSS compliant (9/2013)

Symantec software identifies malicious activity

First FireEye alerts triggered (11/30)

More FireEye alerts triggered (12/2)

DOJ notifies Target (12/12)

Target confirms breach - removes most malware (12/15)

Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18 (12/19)

Target confirms a further 70 million data records stolen (1/10/14)

Attacker Timeline

Attackers steal Fazio credentials

Attackers first breach Target network (11/12)

Attackers test malware on Target POS (11/15–28)

POS malware fully installed

Attackers install data exfiltration malware

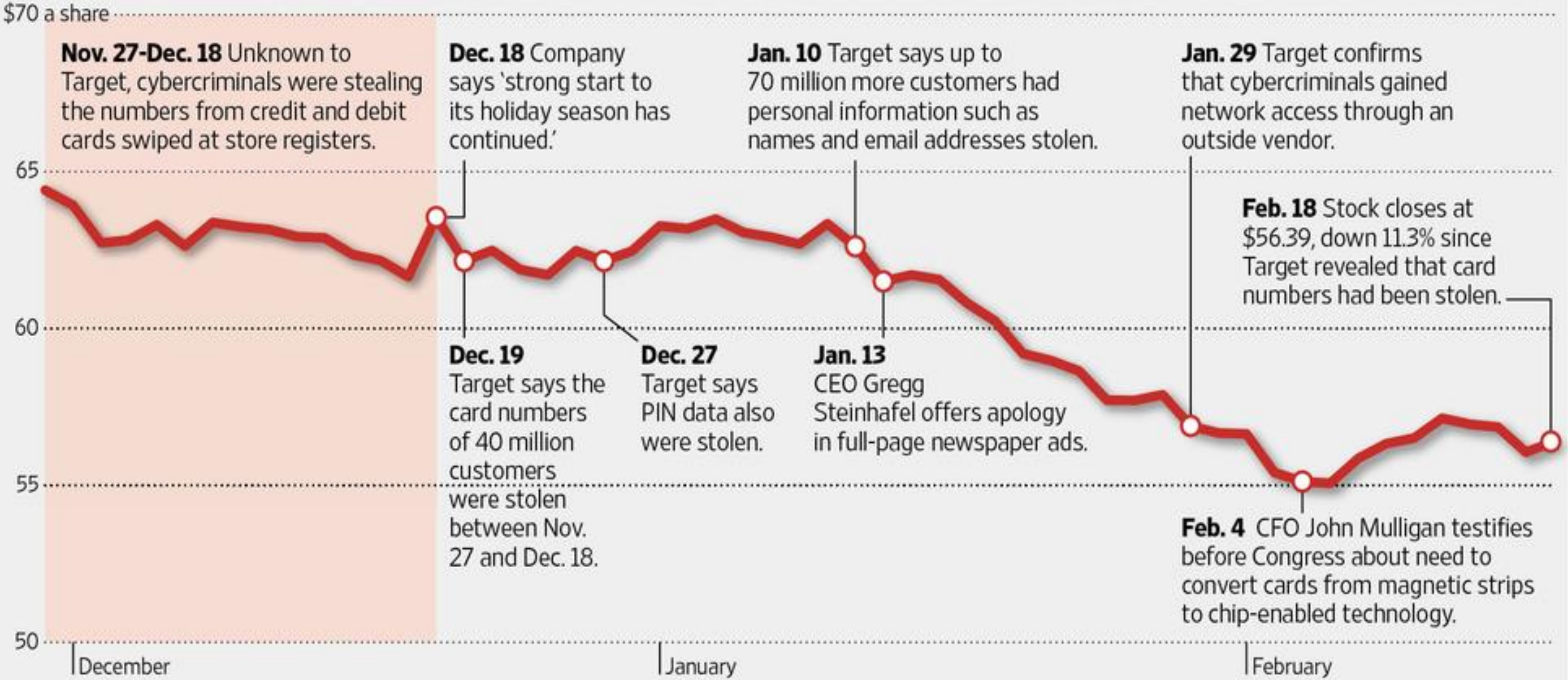
Attackers install upgraded versions of exfiltration malware - begin exfiltrating data

Attackers lose foothold in Target network

Appendix IV

Trying Times

Target's discovery that cybercriminals had stolen the credit and debit card numbers of about 40 million customers led to a series of difficult decisions.



Nov. 27-Dec. 18 Unknown to Target, cybercriminals were stealing the numbers from credit and debit cards swiped at store registers.

Dec. 18 Company says 'strong start to its holiday season has continued.'

Dec. 19 Target says the card numbers of 40 million customers were stolen between Nov. 27 and Dec. 18.

Dec. 27 Target says PIN data also were stolen.

Jan. 10 Target says up to 70 million more customers had personal information such as names and email addresses stolen.

Jan. 13 CEO Gregg Steinhafel offers apology in full-page newspaper ads.

Jan. 29 Target confirms that cybercriminals gained network access through an outside vendor.

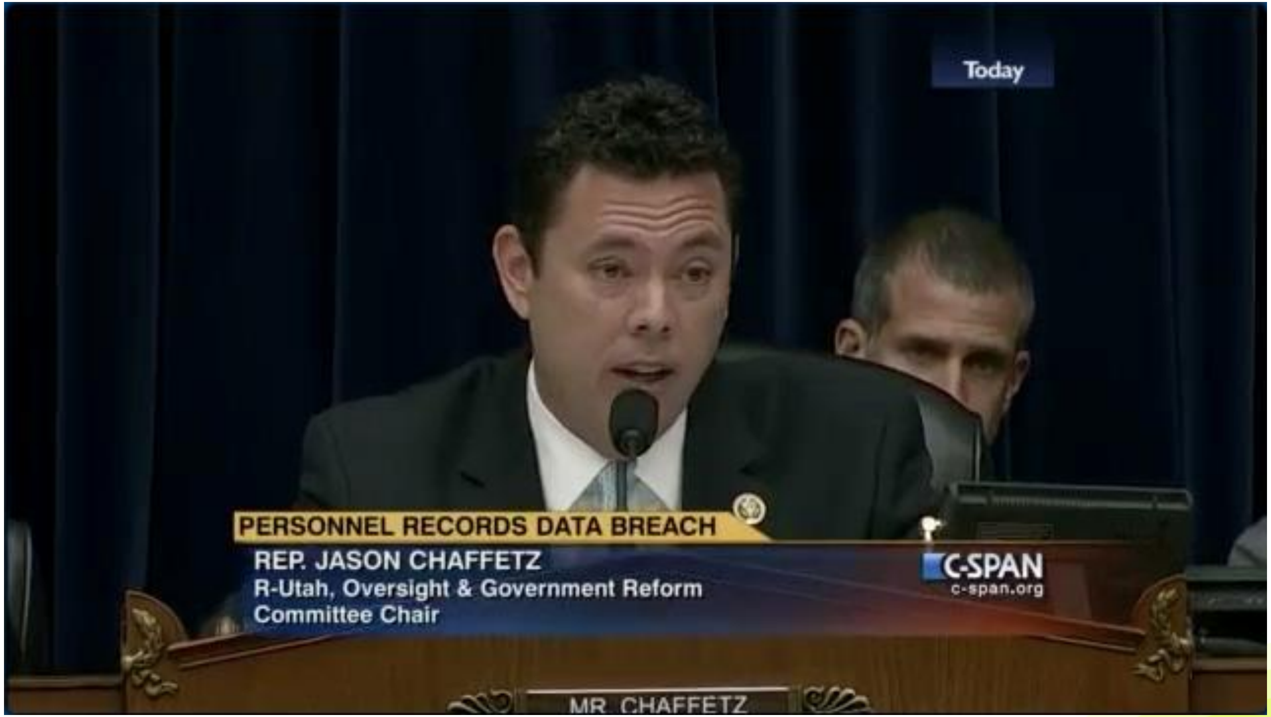
Feb. 4 CFO John Mulligan testifies before Congress about need to convert cards from magnetic strips to chip-enabled technology.

Feb. 18 Stock closes at $56.39, down 11.3% since Target revealed that card numbers had been stolen.

Sources: WSJ Market Data Group; news reports

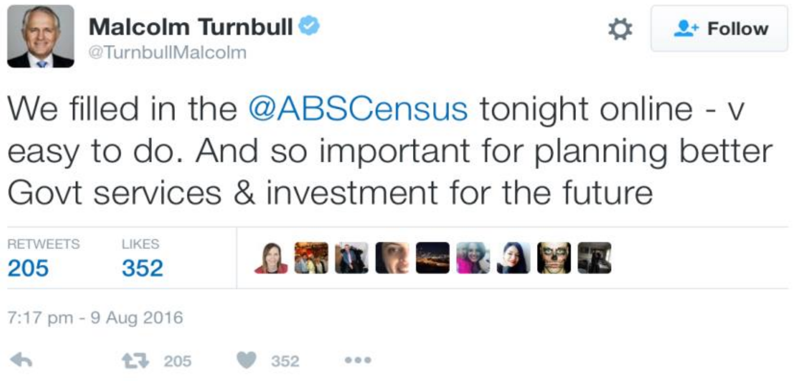
The Wall Street Journal

Office of Personnel Management 2015



Australian Census August 2016

- On 9 August Australia conducted an online census
- The tech savvy Prime Minister even tweeted how easy it was
- Things did not go to plan
- It's another example of how you respond during and after a cyber incident is key



Malcolm Turnbull
@TurnbullMalcolm

We filled in the @ABSCensus tonight online - v easy to do. And so important for planning better Govt services & investment for the future

RETWEETS 205
LIKES 352

7:17 pm - 9 Aug 2016

Crisis Management

Success today depends on:

- Clear thinking and swift action to mitigate reputational damage
- Effectiveness of the table leader who will have overall responsibility for responding to the breach.
- Identify all key stakeholders and ask yourselves what should they know about the crisis and when
- Preparing effective media statements as soon as possible or holding statements as a minimum

Crisis Management Rules

- Never under estimate the potential seriousness of the crisis.
- Speed is essential – fast, effective communications puts you on the front foot.
- Never speculate or lie – be honest and open.
- Only use verified facts and steer clear of opinions.
- Respond ASAP to media/stakeholder enquiries
- Only specifically trained spokespeople should speak to media

Exercise Conduct

- You will work in groups
- Each group will develop responses to an evolving incident
- Exercise injects will be provided as you go along
- Each group will work thru the scenario in their assigned role
- Each group will get a chance to be part of the role plays

EXIT

Disclaimer

- This scenario is entirely fictitious.
- All names, characters, and incidents portrayed in this workshop are fictitious.
- No identification with actual persons (living or deceased), places, buildings, and products is intended or should be inferred.
- Any references to actual international entities or persons is purely for dramatic effect

Our Exercise World: Orangeland

- Orangeland is a 1st World nation in the South Pacific region to the East of New Zealand
- Its capital is Orange City and has a population of 20 million
- It is an advanced high tech economy and advanced governmental structure
- It is a republic with a Presidential Head of State and a Congress of representatives from all over Orangeland

Orange City

Orange City

Orangeland’s Adversary Ruthenia

Groups will Play these Entities

- CertOL: The Federal Government CERT of Orangeland
- Federal Branch of Investigation (FBI): The peak investigative body in Orangeland
- OrangeTel: Orangeland's largest Telco and Internet Company
- Office of the President of Orangeland
- People's Party of Orangeland (PPO): Governing political party
- Orangeland United Party (OUP): Opposition political party
- Clockwork Orange: Orangeland's largest software company
- Orangeland Internet Authority (OIA): Regulator for Orangeland Internet

Group Functions and Tasks

- Groups should appoint four roles:
  - a leader to co-ordinate and give evidence before Congress
  - a spokesperson for the media
  - someone to liaise with other groups to both provide and receive relevant information
  - A scribe to capture all relevant information to inform all activities, all group actions and decisions (maybe with a laptop or good handwriting)
- Each group will needs to prepare a written media briefing document for this incident (no more than 250 words)

Your Table Brief

- Each table has a detailed brief on their role
- All groups are either victims or concerned stakeholders in this breach
- This will be clear as we go on
- Take 5 minutes now to read it as a group and discuss what that might mean in terms of a breach
- Once you have read it decide who will perform the roles of leader, spokesperson, liaison and scribe

Lets begin

- Bring an Open Mind
- Accept the “Scenario Reality”
- Be ready to collaborate with others in your group
- Be ready to play the role you are assigned in front of the entire audience

BREAKING
NEWS
BOB DE LA LANDE
REPORTING

From:. tshields@opo.gov.ol To: tpeters@ppo.org.ol Date: 2016-05-17 15:07 Subject: Re: Masters looking for Options

Tom,
Yes the President is keen to help in any way he can. He made it clear to me and others in the executive office that Masters is unfit to be President or for that matter lead the party. We have lots of information about Masters more crazy ideas from the 1970s and 1980s we you could leak to the media. Seems to me he is getting too easy a run at present. Lets catch up to discuss options in the next few days when you are back in the Orange City.

Terry Shields
Special Counsel to the President
Office of the President of Orangeland

On May 17, 2016, at 10:38 AM, Tom Peters <tpeters@ppo.org.ol> wrote:

Terry,
As previously discussed with you we are looking for better ways to counter Masters. He is killing us at present particularly in the south. What can you guys do?

Tom Peters
National Press Secretary & Deputy Communications Director
Peoples Party of Orangeland

1120
96.1

MR. CLAY
MR. TIERNEY
MRS. MALONEY
MR. CUMMINGS
COUNSEL
MR. MICA
MR. TURNER
MR. WELCH
MR. WOODALL
MRS. LUMMIS
MR. FARENTHOLD

What have we Learnt?

- Communication plans are key in breach situations
- You need to prepare carefully for a breach in terms of people, process and technology
- You need to practice like this regularly
- You can run exercises varying in scope, participants and duration
- You need to embrace the exercise process; use it to identify problems in a safe environment where they can be examined and remedied for future events

Crisis Management Rules

An effective pre-crisis strategy must include:

- Well developed relationships with all sections of the media.
- Holding statements must be prepared and ready to go.
- Key messages and media statements must be simple and free of industry jargon
- The right people for the job – fully supported by executive management.
- A CEO who takes ultimate responsibility for the crisis
- Ignore social media at your peril – but always focus on sections of the media that are running with the story.
- REMEMBER - effective communication protects reputations and determines the course of the crisis.

RSAConference2017