Messaging for a Security Breach

How to Avoid Adding Fuel to the Dumpster Fire

Today's Goal

Gain a basic understanding of what's necessary to help prevent a significant security incident from becoming a memorable, epic, disaster.

Our Approach

- Let’s treat this as a conversation
- Feel free to ask questions as we go

Your Speaker – Ray Strubinger

- Managing Consultant, Digital Forensics & Incident Response at VerSprite
- Background in IT & Information Security Operations
- Certifications in forensics, auditing and incident management
- Led or participated in over 100 cases

What is DFIR?

- Digital Forensics & Incident Response
  - Often used interchangeably – they are different.
- Incident Response – high level activities
  - Processes used to manage, contain & recover from a significant incident.
- Digital Forensics – component of IR
  - Recovery and investigation of material housed on digital media or devices, often in relation to a crime, policy violation, legal or regulatory request.
  - Goal is to determine what happened & ideally lessen the impact of a future occurrence.
  - Tends to be very detailed and technical.

Let's set the stage…

- A company has:
  - Collected vast amounts of sensitive personal data on citizens from many countries
  - A number of systems connected to the internet running a variety of software
  - Software in need of an update
    - (The flaw was made public and a fix was made available)
- Time passes
  - About month after the flaw is announced –
  - Something extremely undesirable happens

Houston, we have a…

- The company announces a breach
  - Company indicates the breach is limited
  - Company mentions they have known about the breach for more than a month
- A breach announcement may not attract much attention
  - People have become somewhat desensitized
    - Every month (or week) there's an announcement about a breach
  - Individual personal impact may not seem significant
    - Little pain from the exposed data – "Oh well, it was just my email address and password"

Any Media Attention is Good, Right?

- The breach announcement drew attention
  - Recall the nature of the business
  - Near comedy of errors ensues
    - Call center struggles under a flood of calls
    - Web sites established to handle inquires are lampooned
    - Company Tweets a rouge website believing it to be its own site
    - Executive profiles are scrubbed from the net

The situation looks grim…

- Executives are summoned to speak to Congress
- Confusing messages & service fees create an uproar
- The scope of the incident expands - twice
- Executives “retire”
- Merriam Webster definition for this type of event

Dumpster Fire

Definition (US, informal)

an utterly calamitous or mismanaged situation or occurrence : disaster

https://www.merriam-webster.com/dictionary/dumpster%20fire

How did things go so wrong?

- Planning, Messaging & Perception
  - What was inferred by the company's actions & statements?
  - Impact on credibility, confidence & competence
- Was this a foreseeable event?
- Was there an established response plan?
- Was there an ability to competently execute the plan?

This doesn't apply to me

- My company is not interesting…
  - Too small
  - Not regulated
  - Not collecting sensitive data
- Conventional wisdom on breaches - not "if" but "when"
- "Is this incident material?"
- Let's assume this does apply
  - Let's talk about what to consider & where to start

Breach announcements

- Level of attention & interest driven by several factors
  - Business Type & Name Recognition
  - Nature & Circumstances of the Incident
  - Magnitude, Impact & Perception of the Incident
  - Messaging about the Incident

How do you start?

- Learn from others
  - Discuss publicly announced security events
    - What would your organization do if in that situation?
    - What type of reception did the announcement receive?
  - Include technical, operations, legal or executive level staff.
  - Include external parties when relevant.

What can be done?

- Understand the business & the risks it faces
  - Types of data collected
    - Is any of the data sensitive?
  - How & where is data stored
    - Is the data a collection of well known file types, contained a database, or captured in a proprietary format?
    - Is the data in the cloud, a company data center or a co-lo facility?
    - Is sensitive data encrypted?
  - Who has access to the data
    - Employees, customers, 3rd parties or anyone?
  - How is the data accessed
    - BYOD, corporate owned and managed devices, any device located anywhere?
  - Are there technical audits or assessments?
    - What's the audit or assessment frequency? Who did the assessment/audit?
    - What were the findings? How did we respond to the findings?

What can be done? (cont.)

- This information is the basis for templates that are customized for the circumstances of the incident
  - Incidents are stressful – be ready before the crisis
  - Plan ahead in case things such as audit findings were not managed properly (ignored) – fix it or take the hit
  - Is there an existing response plan that needs revision?
    - Some of this work may have already been done.
    - What's in the plan?
    - Has the plan been tested recently?

Developing Templates

- Review the information collected from a risk perspective
  - Develop scenarios & determine the likelihood & severity from different ways of losing or exposing data
    - Compromised web site
    - Unprotected cloud storage
    - Lost or stolen laptop or backup
    - Exposure due to phishing
- Build templates to fit scenarios
- Work with counsel – have the templates reviewed so they may be used quickly if the need arise
- Engage specialists

Good artists copy, great artists steal

–Pablo Picasso

What Happened	In November 2016, Uber learned that unauthorized actors obtained access to a private cloud storage environment used by Uber. They accessed stored copies of Uber databases and files. To the best of our knowledge, the unauthorized access began on October 13, 2016 and ended no later than November 15, 2016.
What Information Was Involved	The accessed files contained user information that Uber used to operate the Uber service, including your name and driver's license number. The files included this information for about 600,000 Uber drivers in the United States.
What We Are Doing	We have made changes to our data storage environment and security procedures to decrease the chance of a similar occurrence in the future. To assist you, we are also providing identity theft protection and mitigation services from Experian, including credit monitoring, for twelve (12) months at no cost to you. See details below.
What You Can Do	We recommend enrolling in Experian IdentityWorks℠ and reviewing the additional information below.
For More Information	If you have any questions regarding this incident or if you desire further information or assistance, please contact (844) 439-7669.

https://www.oag.ca.gov/system/files/Sample%20Notice_0.PDF

Good artists copy, great artists steal

–Pablo Picasso

NOTICE OF DATA BREACH

March 29, 2018

To the MyFitnessPal Community:

We are writing to notify you about an issue that may involve your MyFitnessPal account information. We understand that you value your privacy and we take the protection of your information seriously.

What Happened?

On March 25, 2018, we became aware that during February of this year an unauthorized party acquired data associated with MyFitnessPal user accounts.

What Information Was Involved?

The affected information included usernames, email addresses, and hashed passwords - the majority with the hashing function called bcrypt used to secure passwords.

https://content.myfitnesspal.com/security-information/notice.html

What We Are Doing

Once we became aware, we quickly took steps to determine the nature and scope of the issue. We are working with leading data security firms to assist in our investigation. We have also notified and are coordinating with law enforcement authorities.

We are taking steps to protect our community, including the following:

- We are notifying MyFitnessPal users to provide information on how they can protect their data.
- We will be requiring MyFitnessPal users to change their passwords and urge users to do so immediately.
- We continue to monitor for suspicious activity and to coordinate with law enforcement authorities.
- We continue to make enhancements to our systems to detect and prevent unauthorized access to user information.

What You Can Do

We take our obligation to safeguard your personal data very seriously and are alerting you about this issue so you can take steps to help protect your information. We recommend you:

- Change your password for any other account on which you used the same or similar information used for your MyFitnessPal account.
- Review your accounts for suspicious activity.

Prepare for “When”

- Practice to identify potential issues
  - Avoid learning curve challenges during the crisis
- Table top exercises
  - Simulated incidents
    - Testing & assessment of your plan
  - Identify opportunities for improvement

“When” is now

- Long ago: Materials created, approved & kept current
- Time for action
  - How will the announcement be made?
  - Who is the face or signature associated of the announcement?
  - Who else needs to be notified?

Questions?

Ray Strubinger
rays@versprite.com