GJØVIK UNIVERSITY COLLEGE

Security Planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 12.05.14

AGENDA

Crisis Management and Human Factors

- Crisis management
- Post-crisis trauma
- Crisis communication

Wrap-up

- Written exam 28th of May
- Grading

WHAT IS A BUSINESS CRISIS?

A significant business disruption with the direct impact of the lives, health and welfare of an organization and its employees.

Whitman, Mattord and Green

An unstable or crucial time or state of affairs whose outcome will make a decisive difference for better or worse.

Webster's New Collegiate Dictionary

COMMON ELEMENTS TO A CRISIS

- There is a threat to the organization
- There is an element of surprise
- Short decision time
- High probability of news coverage
- Change is the result

CRISIS CATEGORIES

- More smoldering than sudden crises
- Often direct or indirect result of management actions, inactions, or decisions…
- Most common crisis categories:
  - White collar crime
  - Mismanagement
  - Workplace violence
  - Labour dispute
  - Casualty accident

CRISIS MANAGEMENT

- Emergency response
- Crisis communications
- Humanitarian assistance
- Minimize the negative effects on the organization

SYMPTOMS OF POOR CRISIS MANAGEMENT

- Warnings are ignored or played down
- Executives are overwhelmed or cannot respond correctly
- Attempts to keep the crisis quiet
- Quick-fix alternatives look appealing
- Recovery plan lacks focus

PREPARING FOR CRISIS MANAGEMENT

- Prepare contingency plans, identify teams, train staff and rehearse scenarios
- Let it be known that only designated crisis management team members may represent the company
- Plan to react as fast as possible
- Use professional crisis management consultants to review your plans and processes
- Always give the most complete and accurate information possible in any given situation

CRISIS MANAGEMENT TEAM

- Team leader
- Communications coordinator
- Emergency services coordinator
- Other members as needed
- Skill set:
  - Must work well under stress
  - Multitasking
  - Innovative
  - Familiar with operational functions

CRISIS MANAGEMENT CRITICAL SUCCESS FACTORS

- Leadership
- Speed of response
- A robust plan
- Adequate resources
- Funding
- Caring and compassionate response
- Excellent communications

POST-CRISIS TRAUMA

- Posttraumatic stress disorder (PTSD)
  - Psychiatric disorder following life-threatening events
  - Organizations should prepare a humanitarian response, offering counseling services and medical professional care
- It is important that all employees are accounted for before they are released by management
  - Employees in shock should be escorted home or taken care of by emergency services personnel
  - A final information briefing should be held
  - Advise employees to not speak to the media
- Follow up on grieving families and all employees that are injured

CRISIS COMMUNICATION

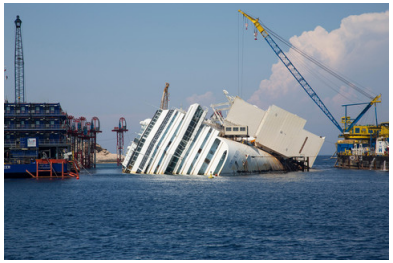
- Communication channels need to be established prior to a crisis
  - Crisis team should be ready
  - Spokesperson (with backup) should be identified and trained
- Understand your audience
- Anticipate the crisis
- Develop holding statements and identify key messages

PUBLIC RELATIONS

- Be first
  - Get the message out to control content and accuracy
- Be right
  - Say and do the right thing
- Be credible
  - Open, honest communication

CASE STUDY: COSTA CONCORDIA

- January 13, 2012: The cruise ship Costa Concordia partially sank after hitting a reef off the Italian cost
  - 30 people dead
  - 2 missing
  - 64 injured



- July 20, 2013: five people working for Costa were found guilty of manslaughter, negligence and shipwreck
  - Roberto Ferrarini (the company's crisis director) received a sentence of two years 10 months
  - The ship's captain Schettino is facing a much harder sentence in a separate ongoing trial, accused for manslaughter, abandoning the ship and causing the loss of the ship

- Example of failed communication strategy: https://www.youtube.com/watch?v=KEyDx5lp-mg

CASE STUDY: THE TARGET DATA BREACH

18 Sources: Target Investigating Data Breach

DEC 13

Nationwide retail giant **Target** is investigating a data breach potentially involving millions of customer credit and debit card records, multiple reliable sources tell KrebsOnSecurity. The sources said the breach appears to have begun on or around Black Friday 2013 — by far the busiest shopping day the year.

Update, Dec. 19: 8:20 a.m. ET: Target released a statement this morning confirming a breach, saying that 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013.

Original story;

According to sources at two different top 10 credit card issuers, the breach extends to nearly all Target locations nationwide, and involves the theft of data stored on the magnetic stripe of cards used at the stores.

TARGET

http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

Dear Guest,

We wanted to make you aware of unauthorized access to Target payment card data. The unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013. Your trust is a top priority for Target, and we deeply regret the inconvenience this may cause. The privacy and protection of our guests' information is a matter we take very seriously and we have worked swiftly to resolve the incident.

We began investigating the incident as soon as we learned of it. We have determined that the information involved in this incident included customer name, credit or debit card number, and the card's expiration date and CVV.

We are partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident and to examine additional measures we can take that would be designed to help prevent incidents of this kind in the future. Additionally, Target alerted authorities and financial institutions immediately after we discovered and confirmed the unauthorized access, and we are putting our full resources behind these efforts.

Yikes! Target's data breach now could affect 110M people

The retailer now says that information taken in December's security lapse includes names, phone numbers, and postal and e-mail addresses, and could affect up to one-third of the US population.

by Don Reisinger | January 10, 2014 11:48 AM PST

639 152 25 +1 190 More + Comments 112

(Credit: Target)

Target's data breach is much broader than once believed

The nationwide retailer on Friday announced t

c|net Like 1.4m Follow @CNET

http://news.cnet.com/8301-1009_3-57617034-83/yikes-targets-data-breach-now-could-affect-110m-people/

06 The Target Breach, By the Numbers

MAY 14

News that **Target's CEO Gregg Steinhafle** is stepping down has prompted a flurry of reports from media outlets trying to recap events since the company announced a data breach on Dec. 19, 2013. Sprinkled throughout those reports were lots of numbers, which got me to thinking about synthesizing them with some of the less-reported numbers associated with this epic breach.

40 million – The number of credit and debit cards thieves stole from Target between Nov. 27 and Dec. 15, 2013.

70 million – The number of records stolen that included the name, address, email address and phone number of Target shoppers.

46 – The percentage drop in profits at Target in the fourth quarter of 2013, compared with the year before.

http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

LESSONS LEARNED FROM THE TARGET BREACH

- Communicate the problem, pronto
- Be ready to respond to your customers
- Push for updated security technology
- Invest in prevention
- Rebuild trust

http://www.forbes.com/sites/sungardas/2014/01/17/five-lessons-for-every-business-from-targets-data-breach/

CASE STUDY: HEARTBLEED

- April 2014: A serious vulnerability was discovered in the widely used OpenSSL library code
  - The Finnish company Codenomicon and NCSC-FI coordinated a responsible disclosure process
  - On April 7 a fix was made available from OpenSSL and the Q&A website heartbleed.com went online
  - The bug even got its own logo!
  - News outlets and social media picked up on this and panic started to spread
  - Many organizations were affected and had to quickly answer questions and reach out to their customers

Status

TUE APR 8TH

SSL Security Update 1 month ago

On 4/7/2014 we were made aware of a critical vulnerability in OpenSSL (CVE-2014-0160), the security library that is widely used across the internet and at Twitter.

We were able to determine that twitter.com and api.twitter.com servers were not affected by this vulnerability.

We are continuing to monitor the situation.

2,025

Tweet

http://status.twitter.com/post/82109064906/ssl-security-update

AWS Services Updated to Address OpenSSL Vulnerability

April 08, 2014

We have reviewed all AWS services for impact for the issue described in CVE-2014-0160 (also known as the Heartbleed bug). With the exception of the services listed below, we have either determined that the services were unaffected or have been able to apply mitigations that do not require customer action.

Elastic Load Balancing: We can confirm that all load balancers affected by the issue described in CVE-2014-0160 have now been updated in all Regions. If you are terminating your SSL connections on your Elastic Load Balancer, you are no longer vulnerable to the Heartbleed bug. As an added precaution, we recommend that you rotate your SSL certificates using the information provided in the Elastic Load Balancing documentation: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/US_UpdatingLoadBalancerSSL.htm

Amazon EC2: Customers using OpenSSL on their own Linux images should update their images in order to protect themselves from the Heartbleed bug described in CVE-2014-0160. Links for instructions on how to update several of the popular Linux offerings can be found below. As an added precaution, we recommend that you rotate any secrets or keys (e.g. your SSL certificates) that were used by the affected OpenSSL process.

Amazon Linux AMI: https://aws.amazon.com/amazon-linux-ami/security-bulletins/ALAS-2014-320/

Red Hat Enterprise Linux: https://rhn.redhat.com/errata/RHSA-2014-0376.html

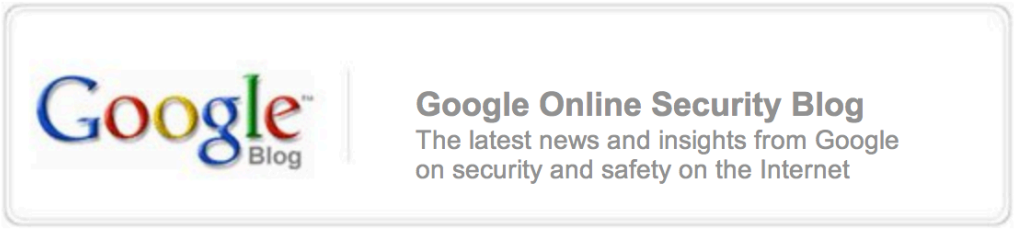
Ubuntu: http://www.ubuntu.com/usn/usn-2165-1/

AWS OpsWorks: To update your OpsWorks-managed instances, run the update_dependencies command for each of your stacks to pick up the latest OpenSSL packages for Ubuntu and Amazon Linux. Newly created OpsWorks instances will install all security updates at boot by default. For more information please see: https://forums.aws.amazon.com/ann.jspa?annID=2429

AWS Elastic Beanstalk: We are working with a small number of customers to assist them in updating their SSL enabled Single Instance Environments that are affected by this bug.

Amazon CloudFront: We have mitigated this issue. As an added precaution, we recommend that you rotate your SSL certificates using the information provided in the CloudFront documentation: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/SecureConnections.html

https://aws.amazon.com/security/security-bulletins/aws-services-updated-to-address-openssl-vulnerability/



Google Services Updated to Address OpenSSL CVE-2014-0160 (the Heartbleed bug)

Wednesday, April 9, 2014 9:58 AM
Posted by Matthew O'Connor, Product Manager

You may have heard of "Heartbleed," a flaw in OpenSSL that could allow the theft of data normally protected by SSL/TLS encryption. We've assessed this vulnerability and applied patches to key Google services such as Search, Gmail, YouTube, Wallet, Play, Drive, Apps, App Engine, AdWords, DoubleClick, Maps, Maps Engine, Earth, Analytics and Tag Manager. Google Chrome and Chrome OS are not affected. We are still working to patch some other Google services. We regularly and proactively look for vulnerabilities like this -- and encourage others to report them -- so that that we can fix software flaws before they are exploited.

If you are a Google Cloud Platform or Google Search Appliance customer, or don't use the latest version of Android, here is what you need to know:

Cloud SQL
We are currently patching Cloud SQL, with the patch rolling out to all instances today and tomorrow. In the meantime, users should use the IP whitelisting function to ensure that only known hosts can access their instances. Please find instructions here.

Google Compute Engine
Customers need to manually update OpenSSL on each running instance or should replace any existing images with versions including an updated OpenSSL. Once updated, each instance should be rebooted to ensure all running processes are using the updated SSL library. Please find instructions here.

Google Search Appliance (GSA)
Engineers have patched GSA and issued notices to customers. More information is available in the Google Enterprise Support Portal.

http://googleonlinesecurity.blogspot.no/2014/04/google-services-updated-to-address.html

Ronald Prins
@cryptoron

Follow

We were able to scrape a Yahoo username & password via the Heartbleed bug. Censored example in our blog:blog.fox-it.com/2014/04/08/ope…

Reply Retweet Favorite More

RETWEETS 64 FAVORITES 8

3:02 PM - 8 Apr 2014

CNET › Security › 'Heartbleed' bug undoes Web encryption, reveals Yahoo passwords

'Heartbleed' bug undoes Web encryption, reveals Yahoo passwords

A flaw in software that's widely used to secure Web communications means that passwords and other highly sensitive data could be exposed. Some say they've already found hundreds of Yahoo passwords.

by **Stephen Shankland** @stshank / April 8, 2014 2:55 AM PDT

http://www.cnet.com/news/heartbleed-bug-undoes-web-encryption-reveals-user-passwords/

Heartbleed test

Enter the hostname of a server to test it for CVE-2014-0160.

yahoo.com Go!

yahoo.com IS VULNERABLE.

Here is some data we pulled from the server memory:

(we put `YELLOW SUBMARINE` there, and it should not have come back)

```
(□uint8) {
 00000000  02 00 79 68 65 61 72 74  62 6c 65 65 64 2e 66 69  |..yheartbleed.fi|
 00000010  6c 69 70 70 6f 2e 69 6f  59 45 4c 4c 4f 57 20 53  |lippo.ioYELLOW S|
 00000020  55 42 4d 41 52 49 4e 45  d8 00 f8 bb a0 d5 d0 6a  |UBMARINE.......j|
 00000030  ff 95 7b 63 0b 6e d8 3c  ab 84 29 c8 29 5a 2e 00  |..{c.n.<..).)Z..|
 00000040  05 00 05 01 00 00 00 00  00 0a 00 08 00 06 00 17  |................|
 00000050  00 18 00 19 00 0b 00 02  01 00 00 0d 00 0a 00 08  |................|
 00000060  04 01 04 03 02 01 02 03  ff 01 00 01 00 77 4e 70  |.............wNp|
 00000070  62 57 46 6e 5a 51 52 30  5a 58 4e 30 52 d2 7f 2d  |bWFnZQR0ZXN0R..-|
 00000080  f6 fa 7d 2e b8 4b bf e3  f8 19 63 87              |..}..K....c.|
}
```

screenshot by Stephen Shankland/CNET; Filippo.io

ashkan soltani
@ashk4n

Following

Ok so Github and OKCupid re-issued SSL certs after #heartbleed but Yahoo, FBI, and OpenSSL have not?! #priorities pic.twitter.com/uVUMpKRSPB

Reply Retweet Favorite More

```
domain:          SSL notBefore:
openssl.org:     Aug 30 10:30:50 2011 GMT
yahoo.com:       Mar 27 00:00:00 2014 GMT
github.com:      Apr  8 00:00:00 2014 GMT
fbi.gov:         Aug  8 16:07:14 2013 GMT
okcupid.com:     Apr  8 20:08:56 2014 GMT
```

RETWEETS 69 FAVORITES 34

4:36 AM - 9 Apr 2014

Flag media

https://twitter.com/ashk4n/status/453723013360648192

LESSONS LEARNED IN CRISIS COMMUNICATION

- **Time is of the Essence**
- **Cover All Your Bases**
- **Structure Messaging Strategically**
  1. Lead with the problem. Explain it as clearly and concisely as possible.
  2. How it impacts the audience specifically. What are the actual and potential ramifications?
  3. Next steps. What are you doing about it? What do they need to do about it? Where can they go to learn more?
  4. Reassure them of your commitment to a resolution, and to them. Let them know who they can contact with questions or concerns.
- **Update As Needed, and Be On-Call for Questions**

http://www.pr2020.com/blog/4-crisis-communication-lessons-from-heartbleed

Never Let a Good Crisis go to Waste: Core Infrastructure Initiative

By Jim Zemlin - April 29, 2014 - 7:15am

Crisis is a difficult thing. In fact, by definition it means *a difficult or dangerous situation that needs serious attention.*

Whether it's an earthquake, multi-car pileup on the freeway or a massive Internet security bug, many times people's first reaction is to ask: How could it have been prevented or detected earlier? As we finished patching our own servers at The Linux Foundation in the wake of the Heartbleed bug, we asked ourselves how we might be able to help prevent this from happening again. Is there a role we can play to help?

That's when we conceived the idea for the Core Infrastructure Initiative (announced last week), which for first time offers a forum where companies and leading open source developers and industry experts can discuss the critical, shared infrastructure that we all depend on. This is not a corporate only effort. We will depend on the developers from the open source community and experts from their respective fields (security as one example) to inform and guide members on where funding is needed most. This is not unlike the neutral framework we've had in place for more than a decade to support Linux and that respects the community norms that make open source successful.

CII intends to support a variety of open source projects that will be identified by members and advisors. Heartbleed was the galvanizing force of the Core Infrastructure Initiative, but we want CII to change reactive responses to a proactive program to identify and fund key developers in essential open source projects. It's also important for us all to face a harsh reality: security threats aren't going away. These threats are a fact of life and all software is vulnerable, whether it's open source or proprietary.

Can CII help minimize the risk of another "Heartbleed?" While security vulnerabilities in our ever more complex software environment are a fact of life, we absolutely hope that by bringing together companies such as Amazon, Cisco, Google, Facebook, Microsoft and more with the developers who work on critical pieces of our infrastructure that we can all help. The idea that open source just happens in someone's basement is a myth. As the software has grown more complex, so has the need for full time developer support. CII will help identify and fund those projects that are critical to our modern computing fabric but that may be under-resourced.

Please join us in this work and support the developers who are building today's most critical infrastructure. Anyone can donate to the Core Infrastructure Initiative at the following link: https://www.linuxfoundation.org/programs/core-infrastructure-initiative#contribute

http://www.linuxfoundation.org/news-media/blogs/browse/2014/04/never-let-good-crisis-go-waste-core-infrastructure-initiative

EXAM

- Written Exam 28th of May
  - 3 hours
  - Different exam for bachelor and master students

- How to prepare?
  - Use the *review questions* in the course text book
  - Review the lecture presentations
  - Read the papers listed on Fronter under *required reading*
  - The Kahoot quizzes are available online (see links on Fronter)
  - *Mock exams* will be published next week

GRADING

Project work accounts for 50% of the grade

- Will be given 0-100 points
- Grade for project work calculated according to the following conversion table:

Grade	Points
A	90-100
B	80-89
C	60-79
D	50-59
E	40-49
F (fail)	0-39

GRADING

Bachelor project work evaluation criteria and points:

Criteria	Points
Scientific content	0-50
Methodology	0-25
Presentation	0-25

Master project work evaluation criteria and points:

Criteria	Points
Scientific content	0-30
Methodology	0-25
Significance and originality	0-20
Presentation	0-25

GRADING

Written exam accounts for 50% of the grade

- *If you fail on the project work you cannot take the exam!*
- The written exam will be given 0-100 points
- Each question on the exam will indicate how many points you may get by providing the correct answer

The **final grade** (project work and exam) will be based upon the points (not grade) of the project work plus the points of the written exam:

Points (final) = (Points (project) + Points (exam))/ 2

The final grade will then be calculated according to the same conversion table as shown previously


GOOD LUCK