

CRISIS COMMS

FOR INCIDENT RESPONSE

INTRODUCTION



SCOTT J ROBERTS

DFIR ENGINEER

@SROBERTS

I WORK FOR GITHUB...



DISCLAIMER:

I AM NOT A PUBLIC RELATIONS SPECIALIST

BUT I CONSULTED A FEW

more than a few actually...

THIS STARTED AS A BLOG POST...¹

¹ <http://sroberts.github.io/2014/09/22/crisis-comms-for-ir/>

**WHAT IS
CRISIS COMMS?**

[...] a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation.

Wikipedia: Crisis Communications



AKA: WHAT YOU SAY WHEN EVERYTHING GOES WRONG.

5 KEYS

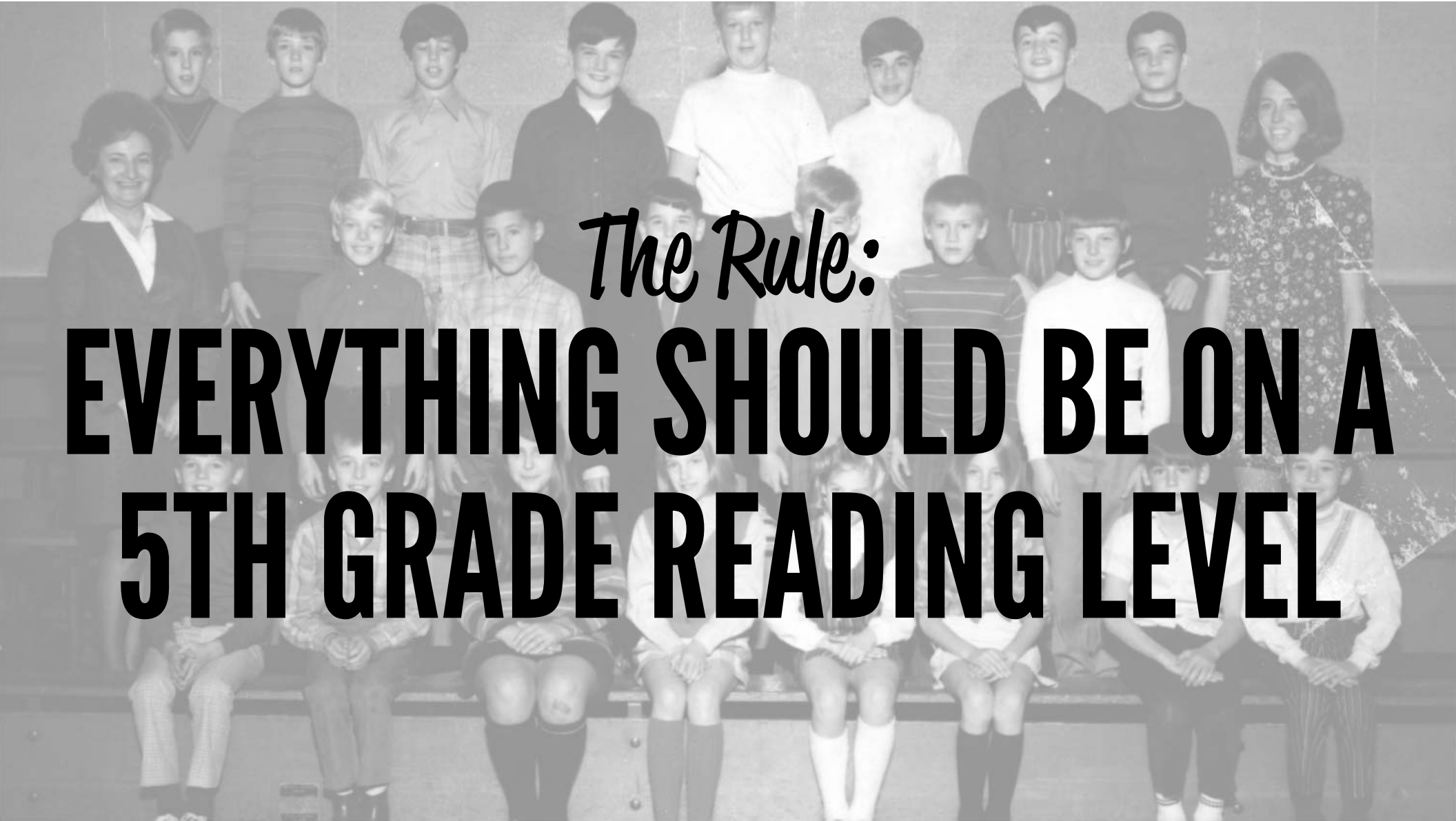
OF IR COMMUNICATION

BE CLEAR

**IT'S DIFFICULT TO
INVESTIGATE INTRUSIONS**

**IT'S DIFFICULT TO EXPLAIN
INTRUSIONS**

IMAGINE BEING NON-DFIR?
OR ONLY SEMI-TECHNICAL?
OR FULLY NON-TECHNICAL?



The Rule:

**EVERYTHING SHOULD BE ON A
5TH GRADE READING LEVEL**

WITHOUT UNDERSTANDING
VICTIMS WILL REMAIN
CONFUSED & CRITICS WILL
REMAIN SKEPTICAL

CLARITY GOES BEYOND ONE MESSAGE
STAY CONSISTENT ACROSS
MESSAGES & MEDIUMS



SO THERE I WAS

ATTRIBUTION

**WORKING WITH THE
EQUATION GROUP GETTING SHELLS**

"You need to be prepared for today's media culture, in which a tweet can become newsworthy and a news interview can become tweet-worthy."

Brad Phillips of Phillips Media Relations

BE TIMELY

TOO EARLY:

**YOU HAVE TO MAKE LOTS OF
FOLLOW-UPS & SEEM OUT OF
CONTROL**

TOO LATE:

**YOUR WARNING IS LESS
ACTIONABLE & YOU SEEM
OBLIVIOUS**

**IN THE END THE BEST OPTION IS OFTEN TO
OVER COMMUNICATE & ASSUME THE WORST**

"IT WASN'T AS BAD AS WE INITIALLY THOUGHT..."

VS.

"ACTUALLY IT'S WORSE THAN WE THOUGHT..."

"The secret of crisis management is not good vs. bad, it's preventing the bad from getting worse."

Andy Gilman of Comm Core Consulting Group

BE ACTIONABLE

**WHAT IS THE ORGANIZATION
DOING TO MITIGATE THE
PROBLEM?**

**WHAT IS THE ORGANIZATION
DOING TO REMEDIATE THE
PROBLEM?**

**HOW CAN PEOPLE IDENTIFY IF
THEY ARE AFFECTED?**

**WHAT IS THE ORGANIZATION
DOING TO PROTECT USERS?**

**HOW CAN PEOPLE PROTECT
THEMSELVES IF THEY ARE
AFFECTED?**

"Next to doing the right thing, the most important thing is to let people know you are doing the right thing."

John D. Rockefeller

BE RESPONSIBLE



This one is scary...

ADMITTING

WHAT WENT WRONG

AND

SAYING YOU ARE SORRY

RESPONSIBILITY TAKES COLLABORATION

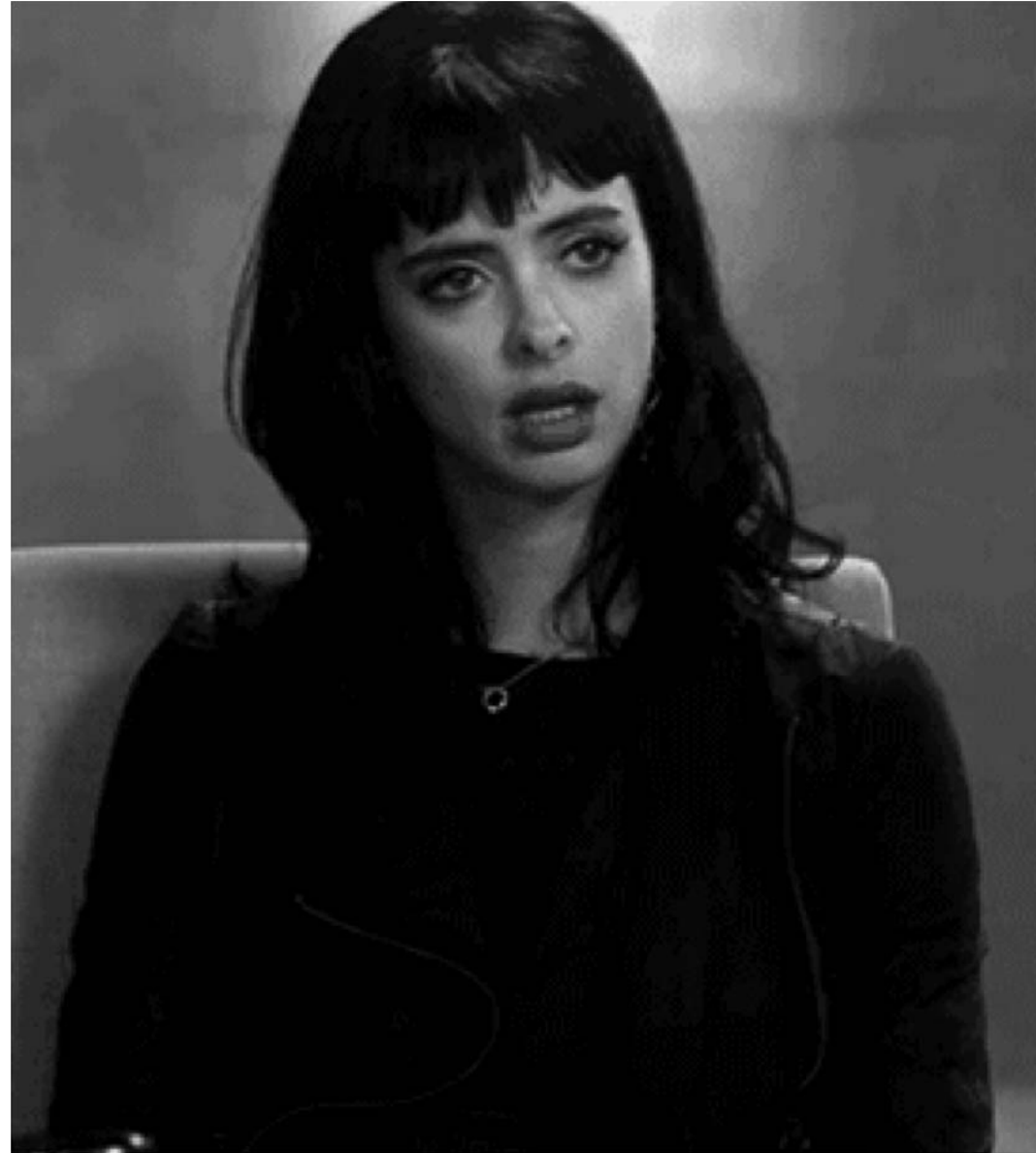
SECURITY TEAM

PUBLIC RELATIONS TEAM

LEGAL TEAM

CUSTOMER SUPPORT

VENDOR NAME DROPPING



"Always acknowledge a fault frankly. This will throw those in authority off their guard and give you opportunity to commit more."

Mark Twain

BE HUMAN

YOU CAN'T OVERVALUE A SENSE OF HUMANITY IN A CRISIS
IT'S WILDLY DIFFICULT & CRITICALLY IMPORTANT



HOW TO SOUND HUMAN

- ▶ Start all communications go through a single person
 - ▶ Avoid Legal-ese & Jargon
- ▶ Say it, write it, read it to yourself, then read it out loud
- ▶ Get outside feedback, but don't sound like a committee

AUDIENCE

EXTERNAL

PRESS, SOCIAL MEDIA, PUBLIC STATEMENTS



EXECUTIVE

FOCUS ON CLARITY, AVOID FUD



INTERNAL

**IF EMPLOYEES DON'T HAVE A MESSAGE
THEY'LL INVENT ONE**

"If you don't tell your story, someone else will."

Unknown

CASE STUDIES



TARGET

VICTIM: CONSUMER RETAIL

ATTACKER: CRIMINAL GROUP

TIMELINE:

- ▶ **??: Intrusion Begins**
- ▶ **Nov. 27 - Dec. 15, 2013: Fraud Takes Place**
- ▶ **Dec. 15, 2013: Breach Confirmed Internally, 40 million cards affected**
 - ▶ **Dec. 18, 2013: Brian Krebs First Article**

TIMELINE (CONT.):

- ▶ **Dec. 19, 2013: Target Acknowledges Breach: Minimal Impact**
- ▶ **Dec. 20, 2013: Target announces "very few"² reports of card fraud**
 - ▶ **Dec. 21, 2013: Banks begin reissuing cards proactively**

² <http://www.wsj.com/news/articles/SB10001424052702304773104579270591741798968>

TIMELINE (CONT.)(YET AGAIN):³

- ▶ **Dec. 27, 2013: 3rd Party IR identifies stolen card/pin information**
- ▶ **Jan. 10, 2014: Access to an additional 70 Million accounts announced**
- ▶ **Jan. 22, 2014: 475 employees from HQ laid off w/700 open recs**

³ <http://blogs.wsj.com/corporate-intelligence/2013/12/27/targets-data-breach-timeline/> & <http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056>

response & resources related to Target's data breach

Visit this page for regular updates and reliable information about our data breach, including all official company communications.



[click here for answers to commonly asked questions about the data breach](#)

Target names Brad

time for smartcards

official documents & communication

We're aware of additional scams that may be perpetrated as a result of our data breach. These links are to all official communication shared by Target. Refer to these if you have questions or concerns about a communication you've received from us.

corporate & leader communications

[website notice to guests \(posted on 12.19.13\)](#)

[Congressional testimony from Target CFO John Mulligan \(shared on 3.26.14\)](#)

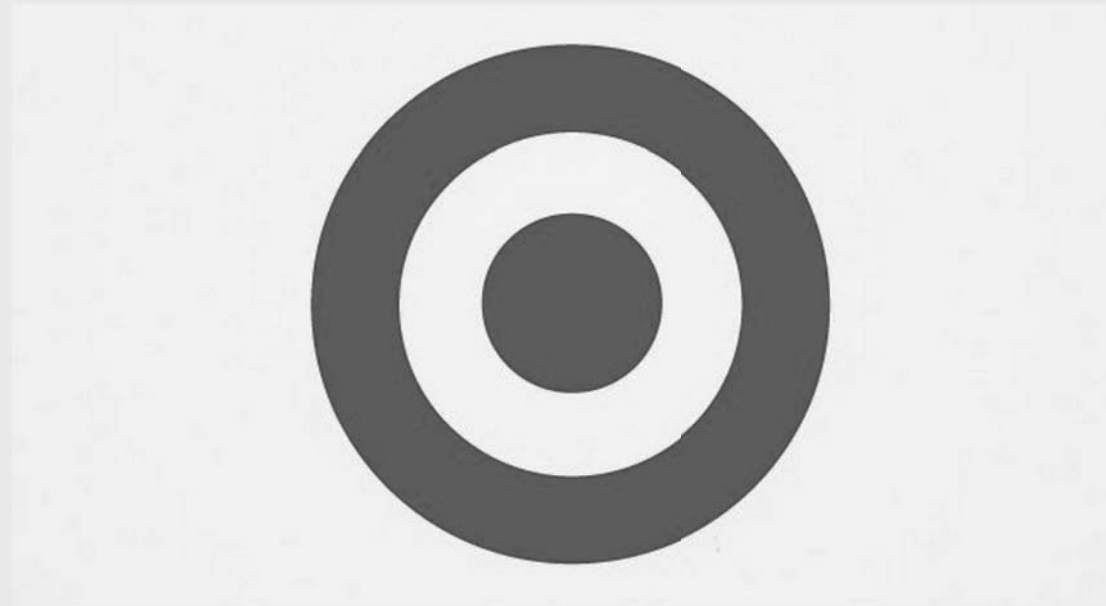
[Congressional testimony from Target CFO John Mulligan \(shared on 2.4.14\)](#)

[a letter from our CEO \(published in newspapers and posted on A Bullseye View on 1.13.14\)](#)

emails to guests & social posts

[email to guests \(begin sending on 1.15.14\)](#)

[email to guests \(sent on 1.13.14\)](#)



an update on our data breach and financial performance



January 10, 2014 Today, Target announced updates on our continuing investigation into the recent data breach and our expected fourth quarter financial performance.

New Details about the Data Breach Investigation

As part of Target's ongoing forensic investigation, it has been determined that

related articles



El papá mejor vestido del mundo: El secreto detrás del estilo de Jorge Bernal para el Día del Padre



World's Best (Dressed) Dad: The Secret Behind Jorge Bernal's Father's Day Style

 HOME > PRESS > RELEASES

Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

Issue has been identified and resolved

MINNEAPOLIS — December 19, 2013

Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.

"Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."

Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.


More information is available at Target's corporate website. Guests who suspect unauthorized activity should contact Target at: 866-852-8680.

About Target



media hotline

We strive to return all of our media inquiries within one business day.

 [email us](#)

 (612) 696-3400

guest relations

[visit Target Help](#)

investor relations

 (612) 696-3400

advertising inquiries

 media@target.com

related content

[Target Provides Update on Data Breach and Financial Performance](#)

[Target Data Security Media Update #4](#)

credit monitoring FAQ

Answers to commonly asked questions about our free credit monitoring offer.

Registration for our free credit monitoring offer ended on April 23.

Because we value you as our guest and your trust is important to us, you can sign up for one year of free credit monitoring that includes identity theft insurance (except where prohibited by law). In addition to a complimentary copy of your credit report, you will receive daily credit monitoring, identity theft insurance where available, and have access to personalized assistance from a highly trained Fraud Resolution Agent. This offer applies to all Target guests who shopped in U.S. stores. To register, please go to creditmonitoring.target.com before April 23, 2014.

In addition, to guard against possible consumer scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Target is also watching out for these scams and working with online partners to take down fraudulent websites and stop social media scams intended to exploit our guests.

Here are some tips:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

You can also find a FAQ specific to the data breach, which includes information related to scams, [here](#).

How to sign up

Who is eligible for free credit monitoring?

If I share my credit or debit account that was used at Target, who should sign up for free credit monitoring?

How do I sign up for free credit monitoring?

additional resources

.....
[answers to questions about the data breach](#)
.....

[response & resources related to the payment card breach](#)
.....

[a message from our CEO related to the payment card breach](#)
.....

[announcement about credit monitoring on A Bullseye View](#)
.....

learn more about Target

.....
[corporate responsibility](#)
.....

[mission & values](#)
.....

[the shopping experience](#)
.....

[investors](#)
.....

[press](#)



Dear Target Guests,

As you have probably heard, Target learned in mid-December that criminals forced their way into our systems, gaining access to guest credit and debit card information. As a part of the ongoing forensic investigation, it was determined last week that certain guest information, including names, mailing addresses, phone numbers or email addresses, was also taken.

Our top priority is taking care of you and helping you feel confident about shopping at Target, and it is our responsibility to protect your information when you shop with us.

We didn't live up to that responsibility, and I am truly sorry

Please know we moved as swiftly as we could to address the problem once it became known, and that we are actively taking steps to respond to your concerns and guard against something like this happening again. Specifically, we have:

1. Closed the access point that the criminals used and removed the malware they left behind.
2. Hired a team of data security experts to investigate how this happened. That effort is ongoing and we are working closely with law enforcement.
3. Communicated that our guests will have zero liability for any fraudulent charges arising from the breach.
4. Offered one year of free credit monitoring and identity theft protection to all Target guests so you can have peace of mind.

In the days ahead, Target will announce a coalition to help educate the public on the dangers of consumer scams. We will also accelerate the conversation—among customers, retailers, the financial community, regulators and others—on adopting newer, more secure technologies that protect consumers.



a message from CEO Gregg Steinhafel about Target's payment card issues



December 20, 2013 Please visit A Bullseye View, Target's online magazine, for video messages from Target CEO Gregg Steinhafel

[watch now](#)

related articles



El papá mejor vestido del mundo: El secreto detrás del estilo de Jorge Bernal para el Día del Padre



World's Best (Dressed) Dad: The Secret Behind Jorge Bernal's Father's Day Style

**AND A BUNCH
MORE...**



BLOG ADVERTISING ABOUT THE AUTHOR

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.

Minneapolis, Minn. based **Target Brands Inc.** has not responded to multiple requests for comment. Representatives from **MasterCard** and **Visa** also could not be immediately reached for comment.

Both sources said the breach was initially thought to have extended from just after Thanksgiving 2013 to Dec. 6. But over the past few days, investigators have unearthed evidence that the breach extended at least an additional week — possibly as far as Dec. 15. According to sources, the breach affected an unknown number of Target customers who shopped at the company's bricks-and-mortar stores during that timeframe.

“The breach window is definitely expanding,” said one anti-fraud analyst at a top ten U.S. bank card issuer who asked to remain anonymous. “We can’t say for sure that all stores were impacted, but we do see customers all over the U.S. that were victimized.”

There are no indications at this time that the breach affected customers who shopped at Target’s online stores. The type of data stolen — also known as “track data” — allows crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe.

Advertisement

Protect your VPN with two-factor authentication.

Your phone is your token! See how at duosecurity.com

My New Book!

SPAM NATION
NEW YORK TIMES BESTSELLER

THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR

BRIAN KREBS

FRONTPAGE OF THE BRILLIANT WINNING STRATEGY WITH KREBSONSECURITY.COM

CLEAR:

4/10

6+ LINKS VS. 1 KREBS ARTICLE...

TIMELY:

4/10

EARLY & OFTEN BACKFIRED...

ACTIONABLE:

3/10

NO IDEA...

RESPONSIBLE:

7/10

DEPENDS WHERE YOU LOOK...

KEY STATEMENT

"Our top priority is taking care of you and helping you feel confident about shopping at Target, and it is our responsibility to protect your information when you shop with us. We didn't live up to that responsibility, and I am truly sorry."

Gregg Steinhafel
CEO of Target

HUMAN:

5/10

CEO WAS GREAT BUT A LOT OF PR...

FINAL SCORE:

48%

A GOOD LEARNING EXPERIENCE...



PENN STATE ENGINEERING

VICTIM: EDUCATION/GOVERNMENT

ATTACKER: NATION STATE

TIMELINE

- ▶ **Unknown: Intrusions 1 & 2 Begin**
 - ▶ **Nov. 21, 2014: FBI Notification**
- ▶ **May 15, 2015: Engineering Network Offline & Statements Released
(Students, Press, & Partners)**
 - ▶ **May 18, 2015: PSU Announces Network Back Online**

Penn State Engineering School Cuts Off Internet After Hacking Attacks



/ SECURITY

Re/code composite image



By Arik Hesseldahl | @ahess247 | EMAIL | ETHICS

May 15, 2015, 11:55 AM PDT

SHARE:



The College of Engineering at Penn State University has cut its connection to the Internet in response to two significant breaches of its systems by hackers, who have, in at least one case, been traced to a group with ties to state-sponsored hackers in China.

The school disclosed the attacks today and said that it had hired Mandiant, the incident response division of the computer security firm FireEye, to help investigate the breach and

<RE/CODE NEWSLETTERS>

- Re/code Daily**
Top stories of the day.
- Re/code Event Updates**
Our signature events sell out quickly. Be amongst the first to know.
- Re/code Product Updates**
Special series, exclusive interviews and new features.

Enter Email Address

SIGN UP

<RE/CODE EVENTS>



Check Out Our Full Calendar Of Events

LEARN MORE

PENN STATE NEWS

Home Research Academics Impact Campus Life Athletics Administration Arts and Entertainment

College of Engineering network disabled in response to sophisticated cyberattack

Plans in place to allow teaching, research in the college to continue as University moves to recover

May 15, 2015

UNIVERSITY PARK, Pa. – The Penn State College of Engineering has been the target of two sophisticated cyberattacks conducted by so-called “advanced persistent threat” actors, University officials announced today. The FireEye cybersecurity forensic unit Mandiant, which was hired by Penn State after the breach was discovered, has confirmed that at least one of the two attacks was carried out by a threat actor based in China, using advanced malware to attack systems in the college.

In a coordinated and deliberate response by Penn State, the College of Engineering’s computer network has been disconnected from the Internet and a large-scale operation to securely recover all systems is underway. Contingency plans are in place to allow engineering faculty, staff and students to continue in as much of their work as possible while significant steps are taken to upgrade affected computer hardware and fortify the network against future attack. The outage is expected to last for several days, and the effects of the recovery will largely be limited to the College of Engineering.

To learn more about the incident, including information for affected faculty, staff and students, visit <http://SecurePennState.psu.edu/>.

What has happened?

On Nov. 21, 2014, Penn State was alerted by the FBI to a cyberattack of unknown origin and scope on the College of Engineering network by an outside entity. As soon as the University became aware of the alleged attack, security experts from Penn State began working immediately to identify the nature of the possible attack and to take appropriate action, including the enlistment of third-party experts, chief among them

SHARE THIS STORY

Tweet



RELATED CONTENT

Internal search opens for associate dean of undergraduate and graduate education

NASCAR’s Jeff Gordon to drive show car on campus, visit Creamery April 14

EcoCAR 3 team members ready for outreach events Jan. 31

TOPICS

Administration

AUDIENCE

Faculty and Staff

Students

CAMPUS

University Park

PENN STATE NEWS

Home Research Academics Impact Campus Life Athletics Administration Arts and Entertainment



President Eric Barron: "This is a new era in the digital age, one that will require even greater vigilance from everyone."

Image: Michelle Bixby

A message from President Barron on cybersecurity

May 15, 2015

Dear Penn State faculty, staff and students,

Today (May 15), University leadership announced that our College of Engineering has been the target of two highly sophisticated cyberattacks. In a coordinated and deliberate response by Penn State, the college's computer network has been disconnected from the Internet and a large-scale operation to securely recover all systems is underway. Our experts expect the network to be back up and running in several days.

While disruptions related to our coordinated recovery will largely be limited to the College of Engineering in the coming days, I feel it is important to reach out to all of you directly. Moving forward, we all will

SHARE THIS STORY

Tweet



RELATED CONTENT

Amidst Legos and rocket attacks, IST student earns online master's degree

Cybersecurity science aims to disarm digital threats

Frequently Asked Questions

Penn State's College of Engineering computer network has been successfully repaired and has returned to service, after being taken offline on May 15 in response to two cyberattacks. The information on this page addresses questions about the situation.

Individuals who receive a PII notification letter can find additional information on the PII Notification page.

QUESTION AND ANSWERS:

> What happened?

On Nov. 21, 2014, Penn State was alerted by the Federal Bureau of Investigation (FBI) to a cyberattack of unknown origin and scope on the College of Engineering network by an outside entity. As soon as the University became aware of the alleged attack, top administrative leadership and experts from Penn State Security Operations and Services, in close coordination with third-party security experts, began working immediately to identify the nature of the possible attack and to take appropriate action. An intensive investigation has been conducted across the College of Engineering computer network and other mission-critical areas of the University since that time.

The investigation revealed the presence of two sophisticated threat actors on the college's network. The FireEye cybersecurity forensic unit Mandiant Corp., a leading cyberthreat recovery firm hired by Penn State after the breach was discovered, has confirmed that at least one of the two attacks was carried out by a threat actor based in China, using custom malware to attack systems in the college and remain undetected on the network.



TRENDING: ObamaCare | Rand Paul | Hillary Clinton | Jeb Bush
SPONSORED: America's Nuclear Energy Future



- NEWS
- POLICY
- REGULATION
- BLOGS
- BUSINESS
- CAMPAIGN
- OPINION
- CONTRIBUTORS
- VIDEO
- PEOPLE
- JOBS
- EVENTS

HOME | POLICY | CYBERSECURITY

Penn State discloses major cyberattack by China



By Elise Viebeck - 05/15/15 02:13 PM EDT

Chinese hackers have spent more than two years combing through Penn State University networks, a breach that might have resulted in intrusions into networks of defense contractors and government agencies.

The university disclosed the breach of its College of Engineering on Friday after the FBI noticed the unusual activity and notified the school in November.

The subsequent investigation revealed that two groups of hackers had been inside the school's networks — one linked to the Chinese government, one likely state-sponsored.

"This was an advanced attack against our College of Engineering by very sophisticated threat actors," Penn State President Eric Barron wrote in a letter to professors and students.

"This is an incredibly serious situation, and we are devoting all necessary resources to help the college recover as quickly as possible."

Universities are attractive targets for Chinese hackers interested in gathering trade and technological secrets from U.S. companies.

Major research schools help develop commercial and defense technology for contractors and the military. Penn State is known for its expertise in aerospace engineering, a topic of major interest to Beijing.

The school hired Mandiant, a top cybersecurity forensics firm, to investigate the attack.

Investigators did not disclose whether the Penn State intruders were able to infiltrate additional networks.

The university notified 500 research partners — including federal agencies and major companies — about possible risks to their networks and has reportedly spent millions of dollars trying to eject the hackers.

This task can prove difficult after even a minor data breach, so there is no telling how long it will take to break hackers' two-year grip on the university's systems.

As part of the effort, technicians are taking the engineering school's network completely offline for several days, according to reports.



NEVER MISS important news from THE HILL

Sign-up for our daily emails and alerts.

Enter Your Email Address

SIGN UP

MORE CYBERSECURITY HEADLINES

Feinstein: Cybersecurity bill now 'in real trouble'

Federal workers union frustrated by OPM hack response

Senators push for extra OPM funding

More Cybersecurity Headlines >
Cybersecurity News RSS feed >

MOST POPULAR

DISCUSSED



Bill would require trade deals to...

A House trade vote could come as soon as this week.



Republicans fear they will win...

Republicans in Congress are worried the Supreme Court will hand them a...



Fast talk from the fast-track...

Some GOP members say that TPA will "constrain the president," but it's...



Obama's frustration with

KEY STATEMENTS

In order to protect the college's network infrastructure as well as critical research data from a malicious attack, it was important that the attackers remained unaware of our efforts to investigate and prepare for a full-scale remediation.

CLEAR:

7/10

YOU JUST NEED TO READ 3 SITES AND...

TIMELY:

7/10

TOOK THEIR TIME *hopefully* **FOR A REASON**

ACTIONABLE:

8/10

NOT MUCH... UNLESS YOU ARE ARL

RESPONSIBLE:

8/10

ONCE YOU FIND IT...

HUMAN:

8/10

ONCE YOU FIND IT... AGAIN...

FINAL SCORE:

76%

A SOLID C WITH A B- AFTER THE CURVE



S

SLACK

VICTIM: SAAS CHAT PROVIDER

ATTACKER: CRIMINAL

TIMELINE

- ▶ **Early February: Incident Began**
- ▶ **Early February: Incident Ongoing Four Days**
 - ▶ **March 27 Web Notification Released**
 - ▶ **March 27 Email Notifications Released**

NEWS

Slack hacked, compromising users' profile data



MORE LIKE THIS



Twitch hit by possible data breach, resets user passwords



Why investors are so excited about Slack

The rise (and rise) of Slack, Silicon Valley's hottest startup

on IDG Answers ➔

How to retrieve data lost from Outlook address book after creating a shortcut?

Credit: Thinkstock



By Zach Miners

FOLLOW

IDG News Service | Mar 27, 2015 12:07 PM PT

RELATED TOPICS

Cloud Computing

Cloud Security

Social Media

The popular group chat tool Slack suffered a hack of its central database last month, the company admitted Friday, potentially compromising users' profile information like log-on data, email addresses and phone numbers.

The database also holds any additional information users may have added to their profiles like their Skype IDs.

The passwords were encrypted using a hashing technique. There was no indication the hackers were able to decrypt the passwords, Slack Technologies said in a blog post. No financial or payment information was accessed or compromised, it said.

The unauthorized access took place over about four days in February. The company said it has made changes to its infrastructure to prevent future

ANDY GREENBERG 03.27.15 2:48 PM

SLACK SAYS IT WAS HACKED, ENABLES TWO-FACTOR AUTHENTICATION

541



THE BUZZY COLLABORATION platform Slack has blown up over the last year, with half a million daily users and a \$2.8 billion valuation. Now it's just hit a different milestone for budding startups: Getting humiliated by hackers who defeated its not-quite-ready-for-primetime security protections.

On Friday Slack announced on its corporate blog that it was hacked over the course of four days in February, and that some number of users' data was compromised. That data included email addresses, usernames, encrypted passwords, and, in some cases, phone numbers and Skype IDs that users had associated with their accounts. The company claims that its passwords were sufficiently scrambled to be unreadable to hackers, but it also admits that it detected "suspicious activity" on a "small number" of Slack user accounts, implying that users' communications were in at least some cases fully accessed by the intruders.

LATEST NEWS



OPEN SOURCE
Google Made Its Secret Blueprint Public to Boost Its Cloud
56 MINS



SILICON VALLEY
VC Firms Aren't Investing in Diversity. It's a Bad Move
56 MINS



ENTERTAINMENT SERIES
WIRED Binge-Watching Guide: Veep
56 MINS



Several People Are Typing

The Official Slack Blog

Follow slackhq **tumblr.**

Jobs Sign In

Go to slack.com

March 2015 Security Incident and the Launch of Two Factor Authentication

Posted [March 27th, 2015](#)

We were recently able to confirm that there was unauthorized access to a Slack database storing user profile information. We have since blocked this unauthorized access and made additional changes to our technical infrastructure to prevent future incidents. We have also released [two factor authentication](#) and we strongly encourage all users to [enable this security feature](#).

We are very aware that our service is essential to many teams. Earning your trust through the operation of a secure service will always be our highest priority. We deeply regret this incident and apologize to you, and to everyone who relies on Slack, for the inconvenience.

Here is some *specific information we can share* about this incident:

FAQ

Q: How do I reset my password?

You can reset your password in your [Slack profile settings](#). In addition, team owners and administrators can now easily reset passwords for an entire team at once using our new [“password kill switch” feature](#).

If your Slack team uses single sign-on (SSO) you do not need to reset your password as we do not store passwords for users with this feature enabled.

Q: Why are you releasing Two Factor Authentication now? Why not earlier?

Two Factor Authentication has been in development for the last few months. It is a complicated change which requires additional support resources, administrative capabilities, changes to all applications, mobile and desktop, and extensive testing. We were about a week from release, with just a few small UI tweaks to simplify and clarify the usage experience.

We have decided to release it immediately, despite the remaining bits of clunky-ness: the feature works and it does provide a significant new level of protection against unauthorized access to your Slack account. We will be improving this feature in future releases but the feature functionality is what is most important right now.

Q: What are you doing to prevent additional breaches?

We cannot overemphasize how seriously we take this incident and the importance we place on the security of your information in the broadest sense, from internal compliance processes, audits and physical access control to continual review of our systems design and approach to technical operations.

Never miss a post! ✕



slackhq

Several People Are Typing

Follow

KEY STATEMENTS

Information contained in this user database was accessible to the hackers during this incident.

&

No financial or payment information was accessed or compromised in this attack.

CLEAR:

9/10

NO VECTOR, BUT OTHERWISE EVERYTHING

TIMELY:

10/10

CONTROLLED BASED ON INVESTIGATION

ACTIONABLE:

10/10

FEATURES & EVERYTHING

You need to sign in to see this page.

Sign in to [#random-slack-channel](#)

Enter your two factor authentication code.

Sign In

Check your authenticator app for your code.
Having trouble finding your code?

If your app is unavailable, use a backup code.

To start using Slack, you'll need to be invited by your team administrator.

Trying to create a team? Sign up on the home page to get started.

FEATURE: TWO FACTOR AUTHENTICATION

- Team Settings
- Manage Your Team
- Invitations
- Billing
- Authentication

- Tour
- Apps
- Brand Guidelines
- Help
- API
- Gateways
- Printing
- Contact
- Feedback
- Our Blog
- Sign Out



SAML authentication

OneLogin, Okta, Bitium, or your custom SAML 2.0 solution is only available on the Plus plan.

Upgrade

Session Duration

Once logged in, users will remain signed in until they explicitly sign out. This setting allows you to force users to log in after a certain amount of time has elapsed since their last login.

expand

Forced Password Reset

You can force a reset of passwords for all team members if you need to. Team members will receive a message from Slack prompting them to visit the reset link via email.

You can also optionally force a password reset for a specific team member. That team member will be signed out of all Slack apps, and they will not be able to log in again until they have changed their password.

close

Sign everyone out of all apps

In order to create a new password, each team member must be able to receive the email we send with the reset link. (Manage your own mail servers?)

Reset Passwords for All Team Members

FEATURE: PASSWORD KILL SWITCH

RESPONSIBLE:

9/10

LIMITED ON MISTAKES, FOCUS ON ACTIONS

HUMAN:

8/10

GOOD WORDS, LIMITED IDENTITY

FINAL SCORE:

94%

Curve Buster!!!

OTHER ORGS DOING THIS WELL

PF CHANG'S

LASTPASS

GITHUB (IMHO)



A WINNER
IS YOU

IN CLOSING

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."

Warren Buffet

MAKE A PLAN

KNOW YOUR **STAKEHOLDERS**

KNOW YOUR **DECISION MAKERS**

KNOW YOUR **METHODS**

KNOW YOUR *Voice*

BE CLEAR

BE TIMELY

BE ACTIONABLE

BE RESPONSIBLE

BE HUMAN

THANKS TO:

- ▶ **Kate Guarente of GitHub**
- ▶ **Rachel Vandernick of WebPageFX**
- ▶ **Kristin Reichardt-Rummell of Swish Media**
 - ▶ **Mark Imbriaco of OperableInc**



@SROBERTS OF GITHUB

ORIGINAL POST: [HTTP://GIT.IO/VKMYC](http://git.io/vkmyc)



THANK YOU!!!





QUESTIONS???