

You've Been Hacked Now What?

Reg Harnish, CISM, CISA, CISSP
Chief Security Strategist
GreyCastle Security

June 5, 2013
NYS Cyber Security Conference

Dear KOR Water Customer,

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your credit card information. On December 21, 2012, KOR was notified by our merchant card provider that a data breach appeared to have occurred on our website and back-office systems. To our knowledge, a part of this breach, your credit card, name and address used at KOR's website (www.korwater.com) may have been compromised. At this time we are still gathering information from the investigation, but we believe the breach occurred sometime between period October to December of 2012.

KOR Water values your privacy and deeply regrets that this incident occurred. Working with law enforcement and forensic investigators, KOR Water is conducting a thorough review of the potentially affected records and computer systems, and will notify you if there are any significant developments. KOR is also cooperating with our merchant provider and the major credit card companies to ensure the incident is properly addressed. KOR Water has implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of our customers.

These measures include:

- immediately securing our back-office systems and internal procedures
- implementing McAfee Secure web scanning services on our web systems
- hiring an independent forensic audit team to research the breach and extent of the incident and review the security of our current systems

We recommend that you closely monitor your credit card for any fraudulent activity, and consider proactively requesting your card company for a replacement. Please know that according to major credit card provider agreements, you are not held liable for any fraudulent purchases that are made using your credit card.

Again, we deeply apologize for this security breach and are taking every step to ensure the security of our web systems and your information. Should you have any questions or concerns, please contact us via the email address security@korwater.com.

Sincerely,



J. Eric Barnes
Co-Founder & CEO
KOR Water, Inc.



 SafeUnsubscribe™

Trusted Email from
Constant Contact

Try it FREE today.

This email was sent to [REDACTED] by stewards@korwater.com |
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).
KOR | 95 Enterprise Ste. 310 | Aliso Viejo | CA | 92656

IMPORTANT INFORMATION

LivingSocial recently experienced a cyber-attack on our computer systems that resulted in unauthorized access to some customer data from our servers. We are actively working with law enforcement to investigate this issue.

The information accessed includes names, email addresses, date of birth for some users, and encrypted passwords – technically 'hashed' and 'salted' passwords. We never store passwords in plain text.

Although your LivingSocial password would be difficult to decode, we want to take every precaution to ensure that your account is secure, so we are expiring your old password and requesting that you create a new one.

For your security, please create a new password for your reg@harnishdigital.com and follow the instructions below.

1. Visit <https://www.livingsocial.com>
2. Click on the "Create New Password" button (top right corner of the homepage)
3. Follow the steps to finish

We also encourage you, for your own personal data security, to consider changing passwords on other sites on which you use the same or similar password(s).

The security of your information is our priority. We always strive to ensure the security of our customer information, and we are redoubling efforts to prevent any issues in the future.

If you have additional questions about this process, the "Create a New Password" button on LivingSocial.com will direct you to a page that has instructions on creating a new password and answers to frequently asked questions.

We are sorry this incident occurred, and we look forward to continuing to introduce you to new and exciting things to do in your community.

Sincerely,
Tim O'Shaughnessy, CEO



Dear Reginald,

We want to let you know that there was a break-in at the VUDU offices on March 24, 2013, and a number of items were stolen, including hard drives.

Our investigation thus far indicates that these hard drives contained customer information, including names, email addresses, postal addresses, phone numbers, account activity, dates of birth and the last four digits of some credit card numbers. It's important to note that the drives did NOT contain full credit card numbers, as we do not store that information. Additionally, please note if you have never set a password on the VUDU site and have only logged in through another site, your password was not on the hard drives.

While the stolen hard drives included VUDU account passwords, those passwords were encrypted. We believe it would be difficult to break the password encryption, but we can't rule out that possibility given the circumstances of this theft. It's best to be proactive and ask that you be proactive as well.

SECURITY PRECAUTIONS:

If you had a password set on the VUDU site, we have taken the precaution and resetting that password. To create a new password, go to www.vudu.com, click the "Sign In" button at the top of the page. Enter your current username and password when prompted, then follow the instructions to reset your password securely. Also, if you use your expired VUDU password on any other sites, we recommend that you change it on those sites as well.



As always, remember that VUDU will never ask you for personal or account information in an e-mail. Please use caution if you receive any emails or phone calls asking for personal information or directing you to a web site where you are asked to provide personal information.

As an added precaution, we are arranging to have AllClear ID protect your identity for one year at no cost to you. We have [FAQs](#) on our web site (vudu.com/passwordreset) to answer questions on the incident and to more fully describe how to use the AllClear ID service. We have reported this incident to law enforcement and are cooperating fully with their investigation. We want you to know that we take this matter very seriously, and we apologize for any inconvenience this may have caused you.

Thank you,

Prasanna Ganesan
Chief Technology Officer, VUDU

Comparing Responses



techvalley
COMMUNICATIONS

 **BEST**
CLEANERS

CONFIDENTIAL

Audience Survey



1. Do your organization have
an Incident Response Plan?



Audience Survey



2. If yes, has your plan been
tested?



Audience Survey



3. If yes to 1 and 2, are you confident that your plan **will be effective in the event of a real incident?**



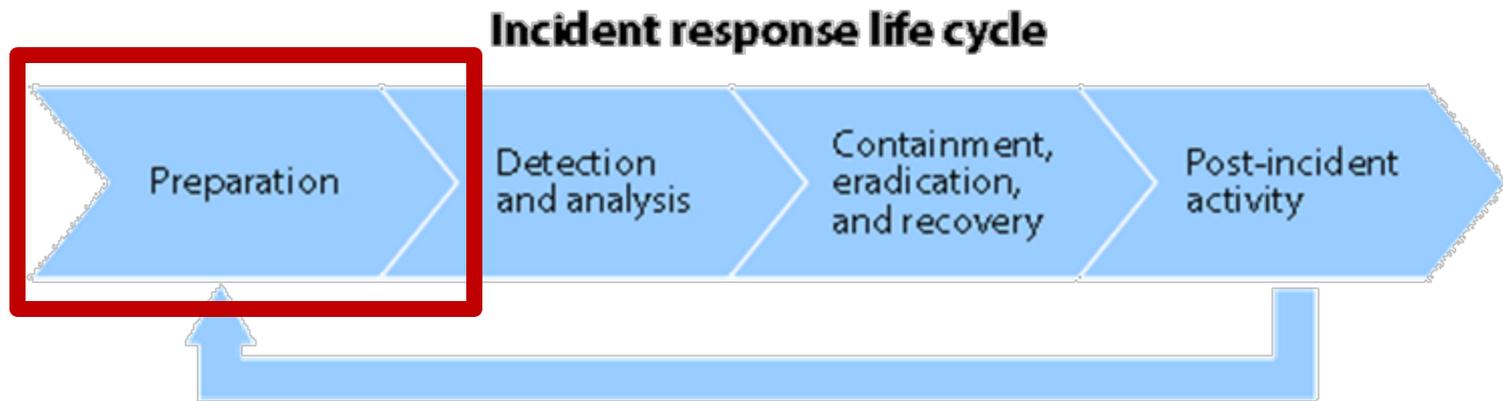
You've Been Hacked – Planning for Failure

Just don't.



Put your response capabilities where your critical assets are

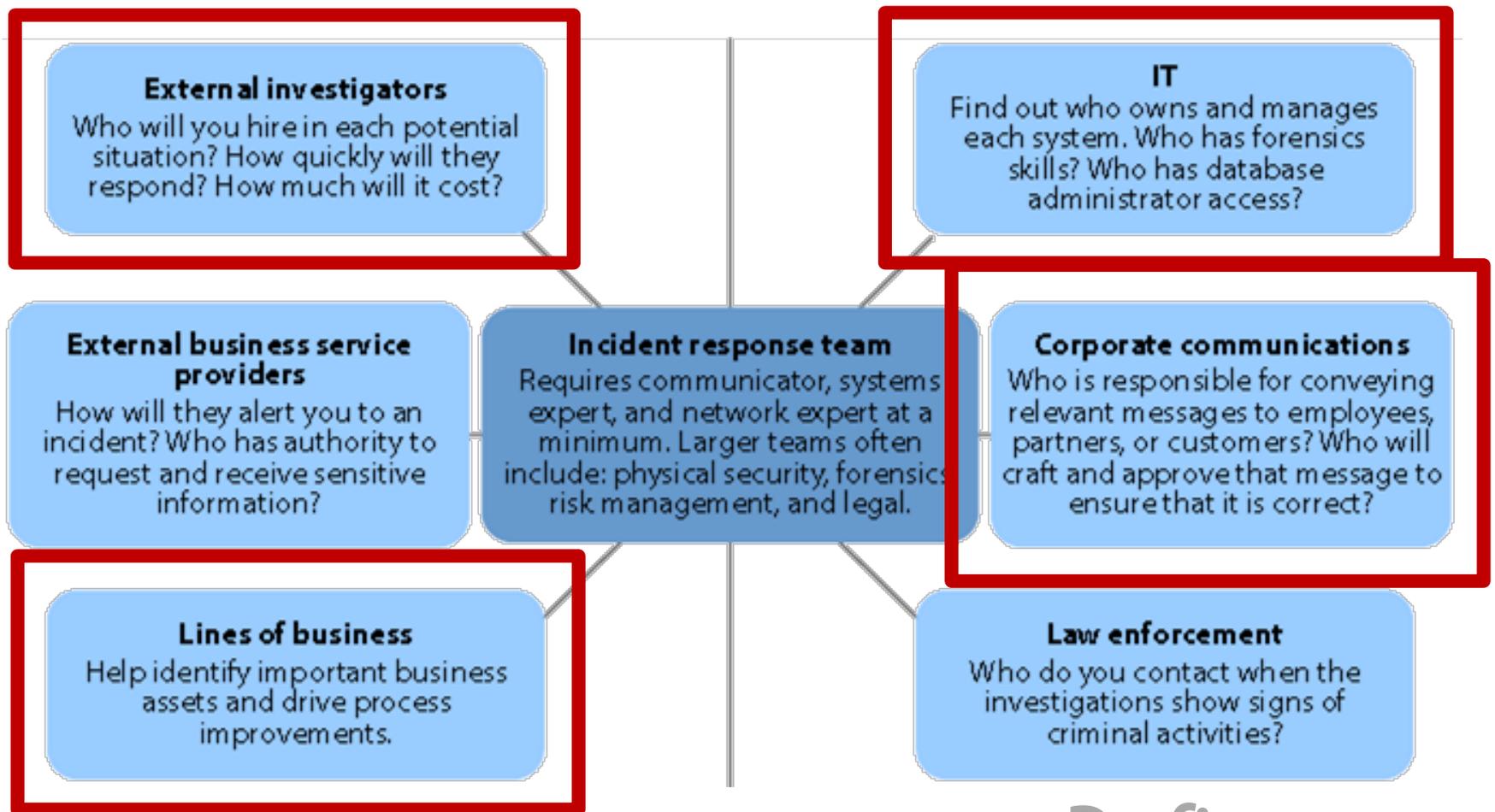




Develop your
Incident Response Plan (IRP)

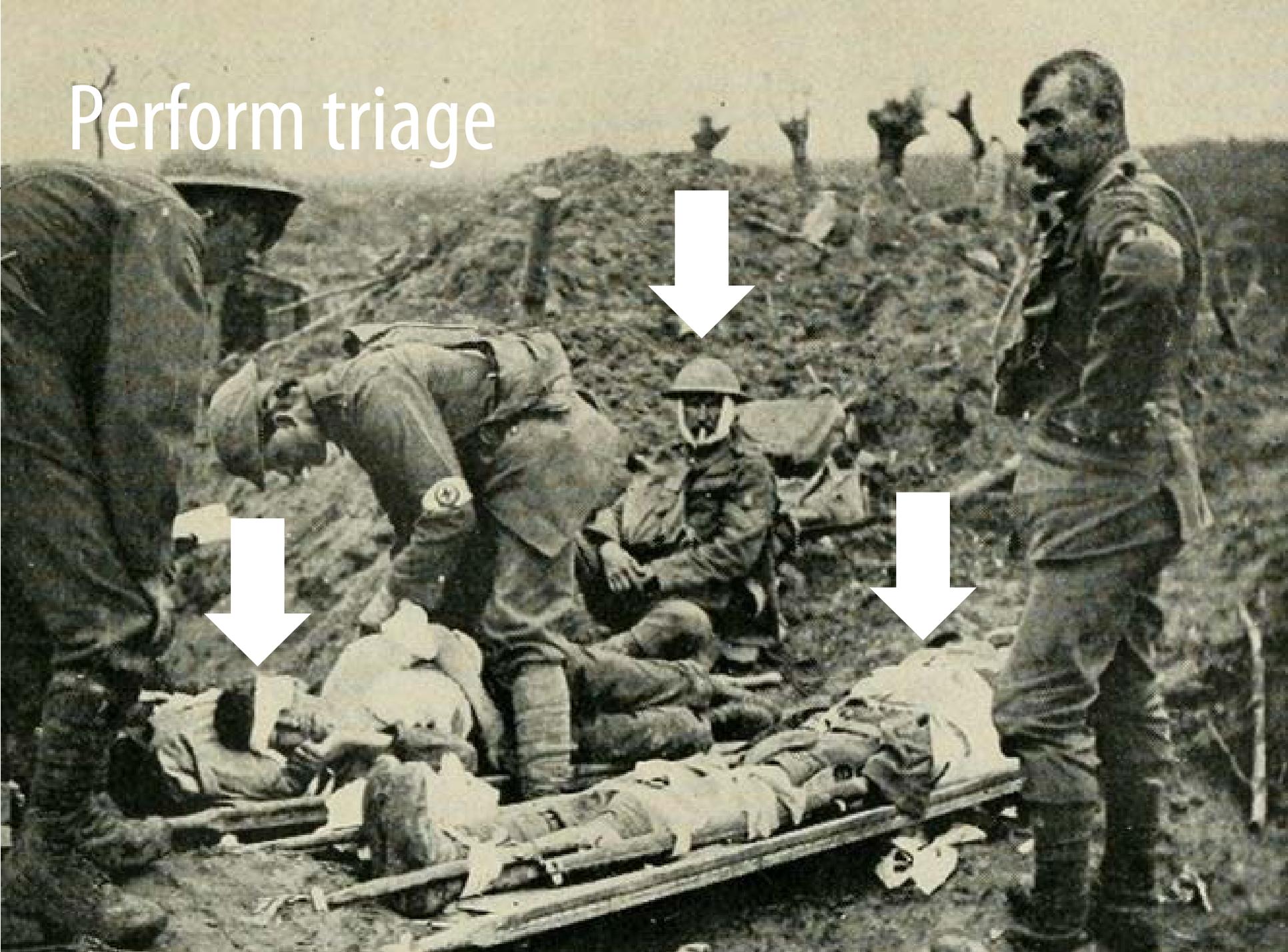
Build your Incident Response Team (IRT)





Define your Incident Management Team

Perform triage



Forensics

- Decide early if you're going to litigate
- Forensics is not just bagging and tagging
- Record everything
- Make sure you're logging
- Establish secure storage location(s)
- Leave it to the experts



Don't touch **anything**



Compliance



- Understand your reporting requirements
 - 46 states and the Feds require reporting
 - NYS Information Security Breach and Notification Act
 - HIPAA HITECH, PCI, NERC CIP
 - Encryption, datatypes and volume change reporting requirements
 - “Reasonable” is basically undefined
- Use a recognized industry framework



Testing and Training



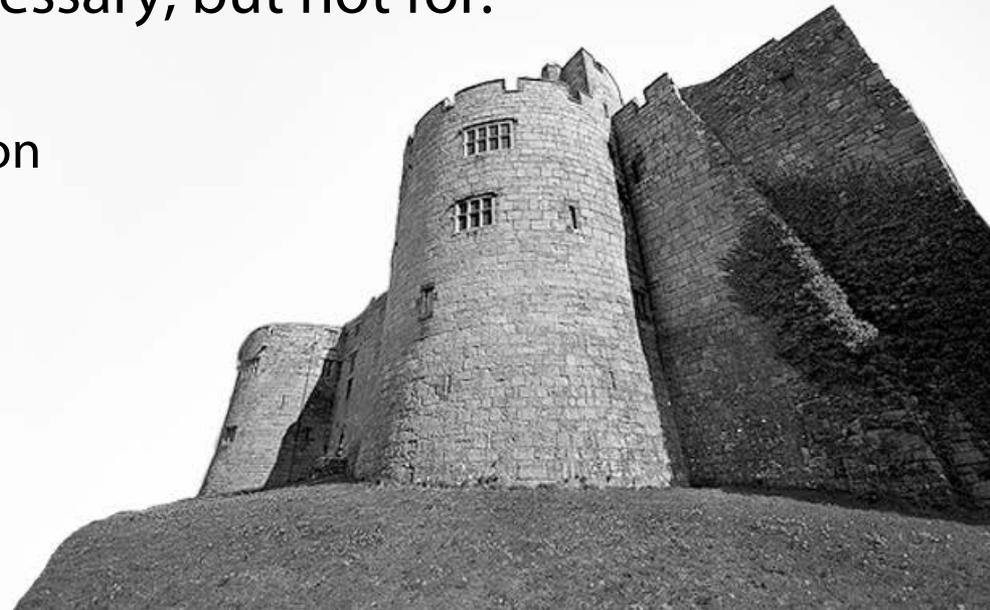
- If you don't test, your plan isn't prepared
- If you don't train, your people aren't prepared
- Train early and often
 - Table-topping
 - Simulations
- Budget for testing and training
- "A good shooter can make a bad gun shoot well"



Outsourcing



- Don't be afraid to outsource, particularly for:
 - Forensics
 - Legal counsel
 - Public Relations
 - Tasks where specialized expertise is required
- Leverage experts where necessary, but not for:
 - Incident reporting
 - Incident Response coordination
- You can't outsource liability



Don't go on the offensive



You've Been Hacked – Lessons Learned

Lessons - Legal

- Be prepared for litigation
- Allow your legal team to drive data retention and destruction requirements
- Decide if you plan to litigate before you respond
- Understand Cyber Liability Insurance – what it is and what it isn't



FIVE GUYS®
BURGERS and FRIES



Lessons – Public Relations

- Know what to say, who to say it to, and when to say it
- Learn the definition of “reasonable”
- Handle information leaks
- Develop communications templates

The
Desmond
Hotel & Conference Center

You've Been Hacked – Incident Response Standards

Standards in Incident Response



NIST

**National Institute of
Standards and Technology**
U.S. Department of Commerce



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

 **GreyCastle**
security



Standards in Incident Response



- NIST Computer Security Incident Handling Guide
<http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>
- US-CERT Handbook for Computer Security Incident Response Teams (CSIRTs)
www.cert.org/archive/pdf/csirt-handbook.pdf
- ENISA Incident Handling Process
<http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process>



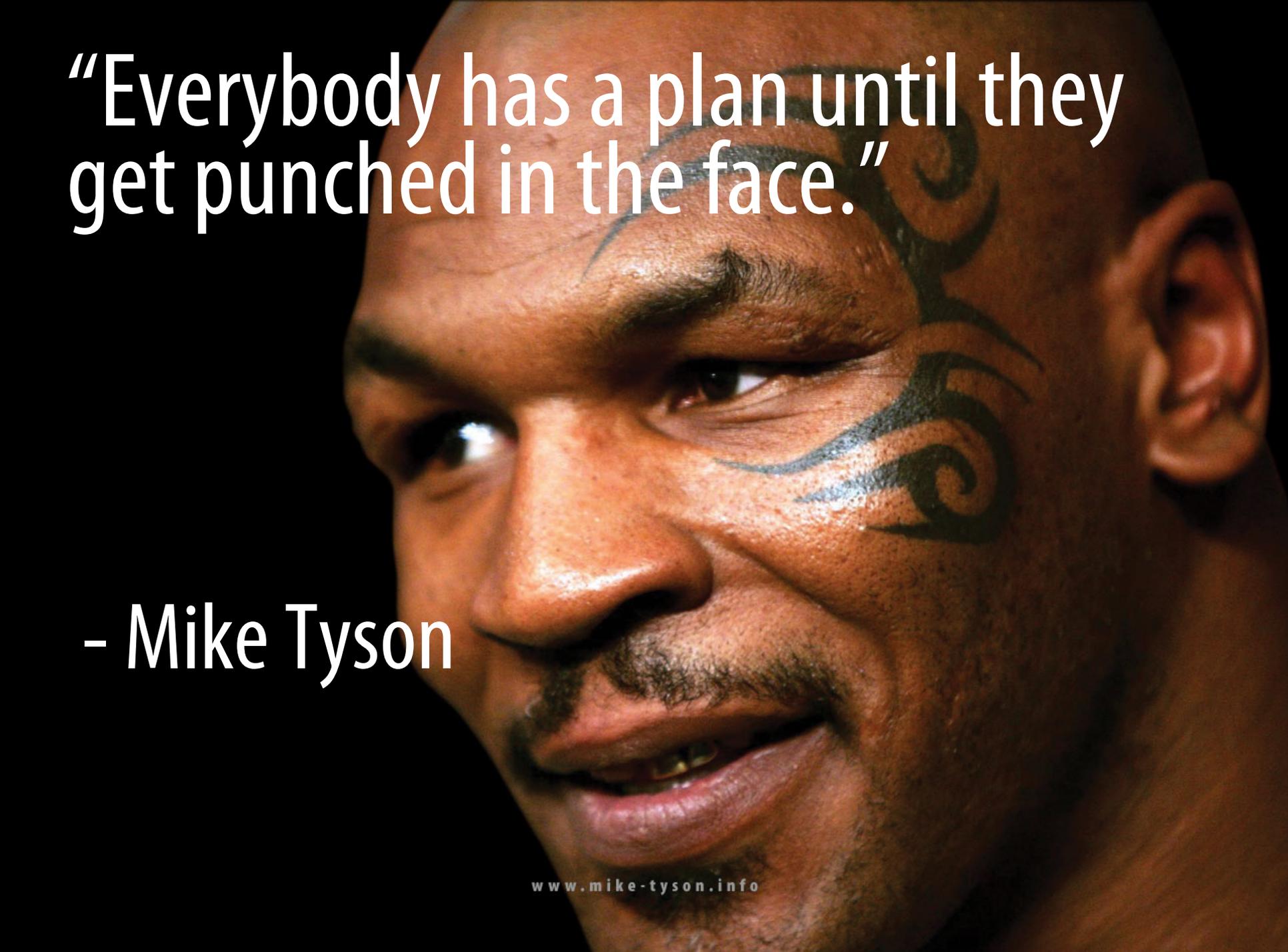
Reporting an Incident



- Internet Crime Complaint Center – www.ic3.gov
- Federal Bureau of Investigation – www.fbi.gov
- Information Sharing and Analysis Center(s)
- Local Police – 911



Final Thoughts

A close-up, high-contrast photograph of Mike Tyson's face. He is looking slightly to the left of the camera with a neutral expression. He has several prominent black tattoos on his face, including a large one on his forehead and another on his right cheek. The lighting is dramatic, highlighting the texture of his skin and the details of his tattoos.

“Everybody has a plan until they
get punched in the face.”

- Mike Tyson

“We’ve been on a lot of adventures together, and it seems like you haven’t learned anything.

Anything.”

- Alan

The image features a hand reaching upwards on the right side, set against a background of numerous question marks. The background has a warm, textured color palette of orange, yellow, and green. The text 'GOT QUESTIONS?' is prominently displayed in the center-left area.

**GOT
QUESTIONS?**



twitter.com/greycastlesec
blog.greycastlesecurity.com