



Hacks, Flacks and Attacks: Collaborating on Risk Communications Before, During and After a Breach

HARLAN LOEB
EDELMAN

Session ID: DAS-401

Session Classification: Intermediate

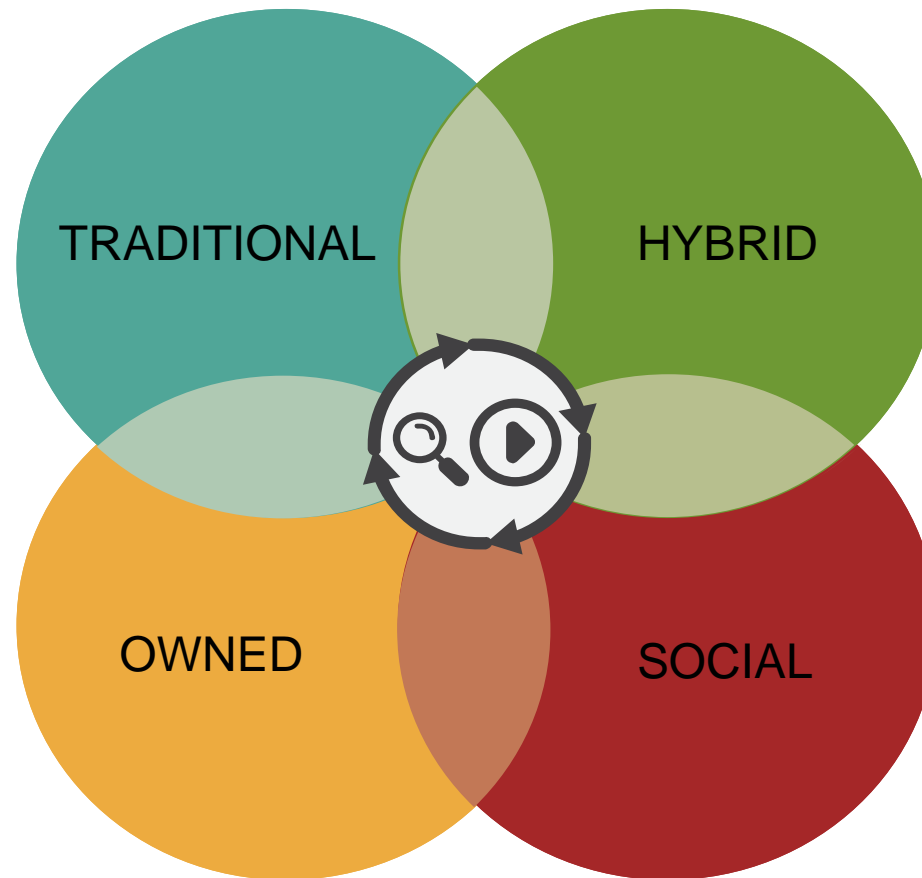
RSACONFERENCE2012

Session Goals & Introduction

- Provide insight into the importance of communications in avoiding/dealing with security incidents
- Outline the elements of a successful communications response to an incident
- Share practical guidance for the security professional related to PR, including working with the communications team
- Action: Take informal poll of attendees on if they have an incident response plan in place. Follow up and ask how many have communications as part of that plan.



3 Things Every CSO Must Know About Crisis



Security Incidents Draw Public Scrutiny

TechCrunch

**Zappos Suffers Security Breach;
Customer Emails And
Passwords Affected**

SOFTPEDIA®
Updated one minute ago

**Anonymous Launches DDoS Attack
on CapitalOne**

ZDNet

**Sony's data breach costs likely to
scream higher**

**infosec
ISLAND**

**Fallout from the
Christmas Hack of Stratfor**

**USA
TODAY**

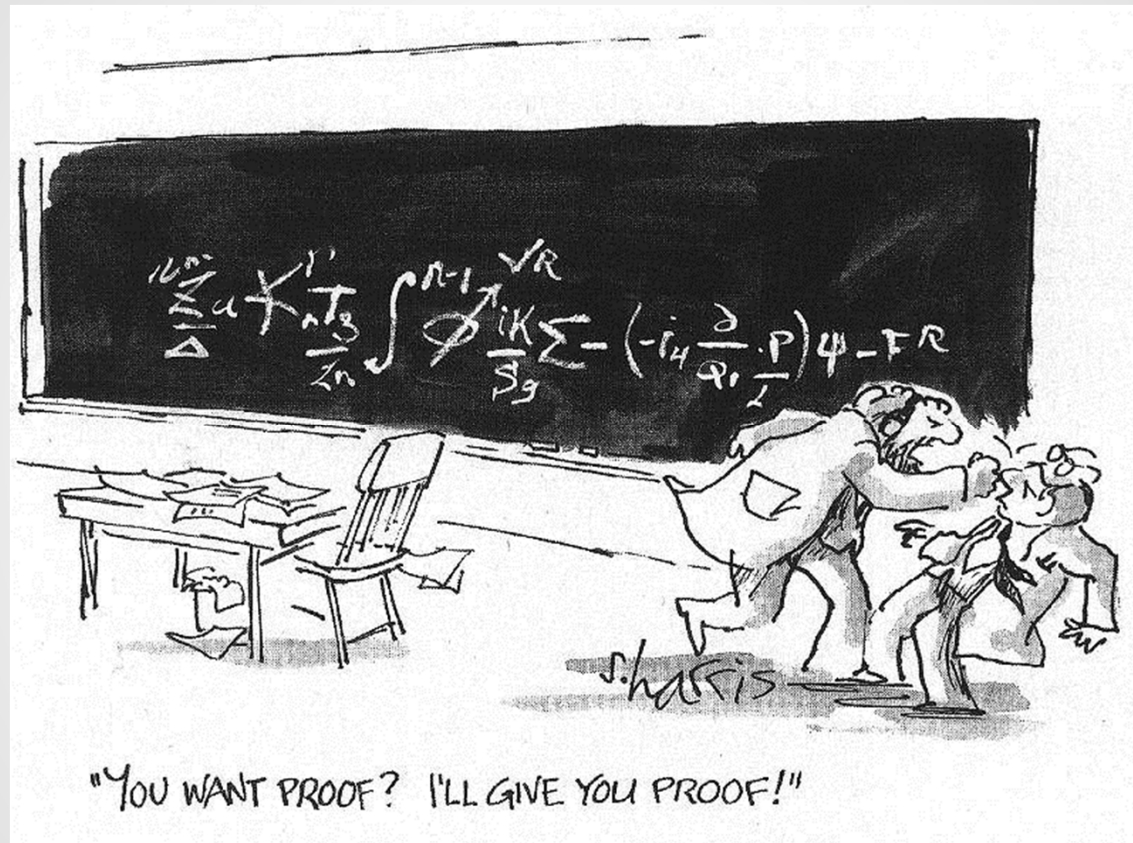
**Citigroup latest to report
data breach**

Bloomberg

**Patient Data Breaches Surge as Hospitals
Scrimp on Security**



A Communications Imperative: Show Your Work



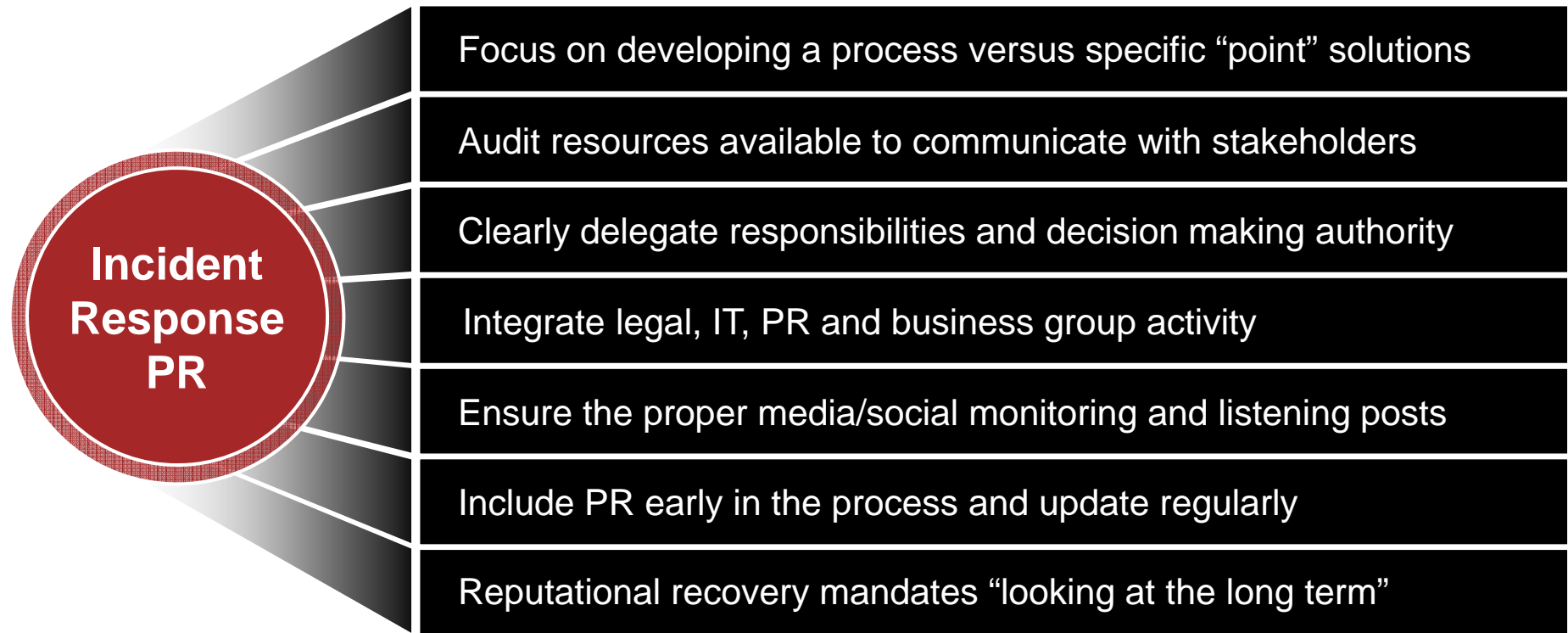
Challenges with Communications During an Incident



Crisis Preparation Mindset & Conflicting Orientation



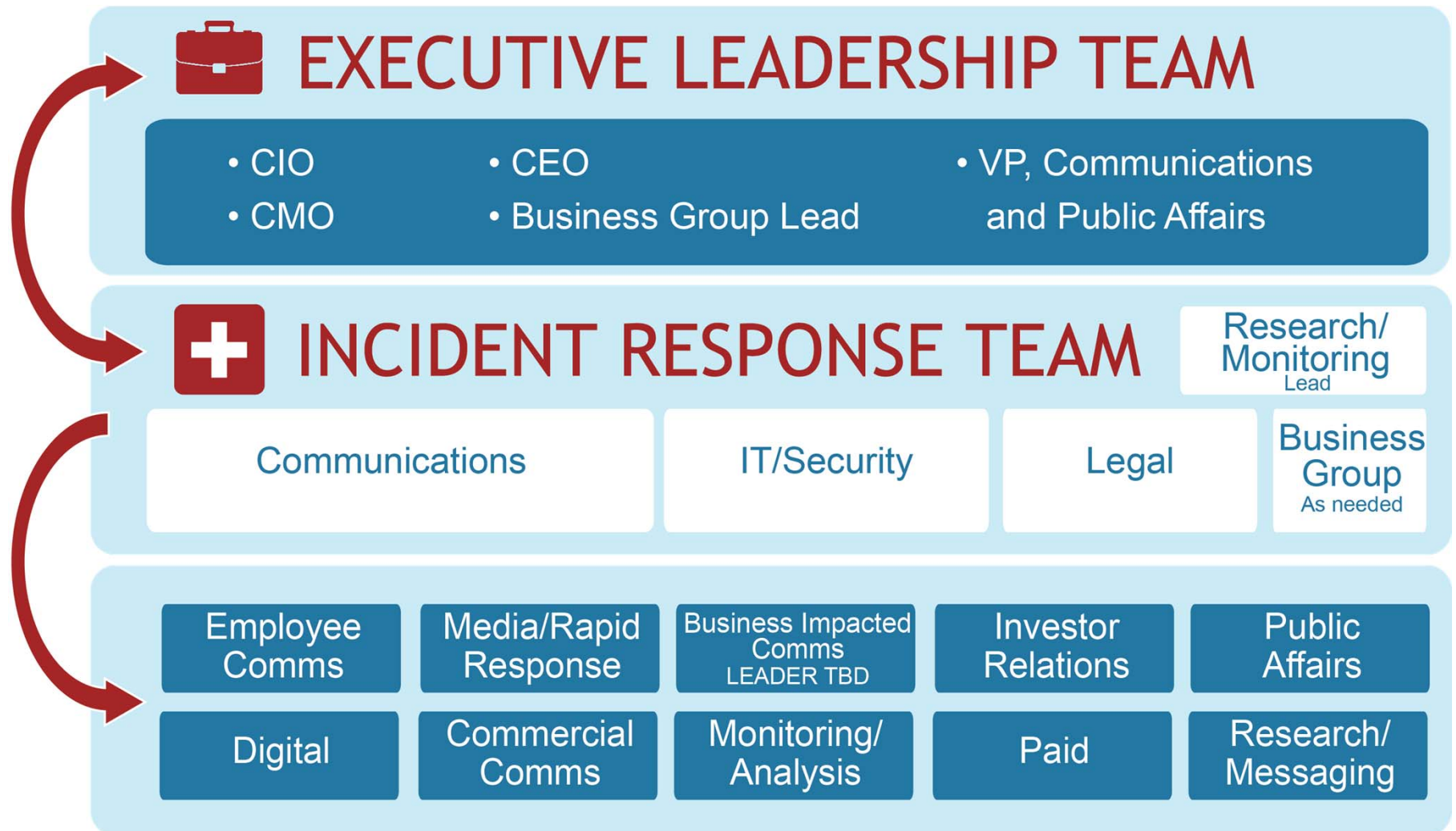
An Approach to Information Security Communications



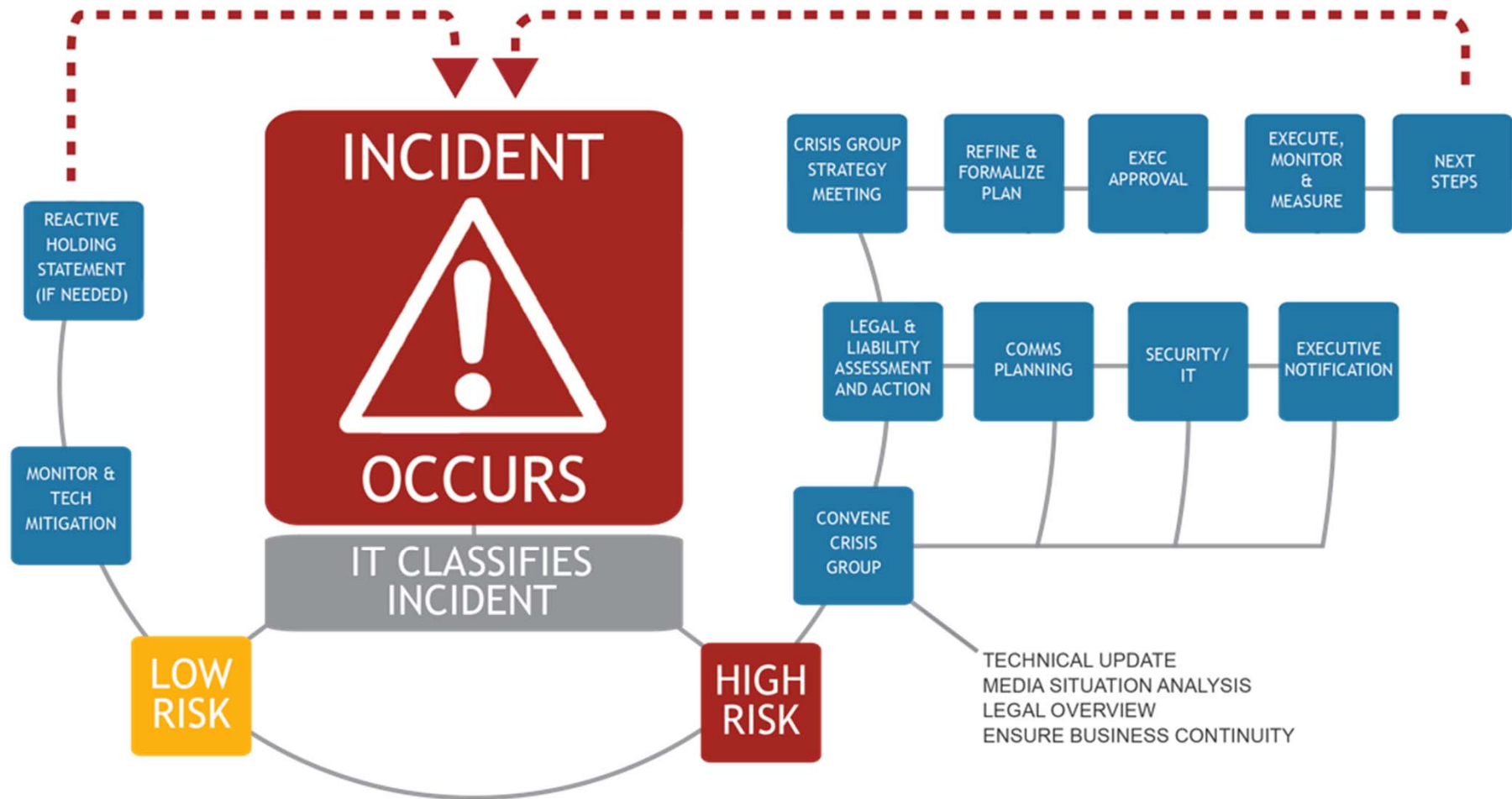
An Effective Immediate Response



Communications Incident Organization



Communications Response Framework



Sample Scenario Overview



BRIEF

- Company X notices strange activity in its IT environment but is yet unsure what if any information was compromised.
- Days later hacktivists claim to have stolen confidential customer data and post it on the Internet and spread via social media channels .
- There is immediate media attention and inquiries, as well as calls from regulatory bodies about the hacktavists' claims.



APPROACH

- Immediately issue holding statement acknowledging the incident, that it's under investigation and detail on the scope of information lost (if known).
- Work with legal to determine formal notification requirements .
- Inform consumers about incident, safeguards and actions to mitigate any fraud.
 - Formal letter and e-mail
 - Set up a phone/email contact hotline for consumers
- Provide additional information through appropriate channels reiterating commitment to customer protection, the type of information lost and steps being taken.
- Consider targeted media engagement with senior executive once issue is contained.
- Refrain from direct engagement with hacktivists.

Likely Primary Audiences and Stakeholders

- Customers
- Employees
- Law enforcement
- State and federal regulators

Holding Statement Other Potential Actions/Materials

- Executive Q&A
- Media and social monitoring
- Landing page with additional information
- Long-term reputation planning



Case Study: Sony PlayStation Network Breach



Case Study: Sony PlayStation 2.0

PROMPT NOTICE VIA BLOG



The screenshot shows the PlayStation.Blog interface. At the top, it says 'PlayStation.Blog' with a PS3 icon and a dropdown menu. Below this, there's a post by Philip Reitering, SVP & Chief Information Security Officer, dated October 11, 2011. The post title is 'An Important Message From Sony's Chief Information Security Officer'. Below the post, there are two comments: one from 'pitythefool852' saying 'Best Sony security response ever.' and another from 'KazeEternal' saying 'Thank you for the update. Please keep up the good work.'

MORE NEUTRAL COVERAGE



The screenshot shows the threatpost website. The article is titled 'Sony Detects Suspicious Behavior, Locks 93,000 Online Accounts' by Brian Donohue, dated October 12, 2011, 9:27AM. The article text states: 'Sony locked the accounts of some 93,000 individuals on the Playstation Network (PSN), the Sony Entertainment Network (SEN), and Sony Online Entertainment (SOE) services following a mass log-in attempt using username-password combinations obtained from an unnamed source. The attack affected less than one tenth of a percent of PSN, SEN, and SOE user bases combined, and the majority of log-in attempts failed. However, the 93,000 accounts that Sony ended up locking out were compromised, the company said. According to a statement put out by Sony's CISO, Philip Reitering, only a small fraction of the 93,000 compromised accounts showed activity before being locked. Reitering's statement claims that the username-password data-set tested against the networks must have come from some outside site, source, or company, as the vast majority of these attempts failed. Presumably, those attempts that did succeed occurred in cases where users recycled their username-password combos with some other compromised source.'



Case Study: RSA



Guidance for the Security Professional



Benefits of an Integrated Response



Good Communications Can Help Prevent an Incident



How to Apply What You Learned Today

- In the first three months following this presentation you should:
 - Speak with your communications/PR team to evaluate existing security incident response plans
 - Identify a team of key stakeholders from legal, IT and communication and develop clear roles/lines of authority ahead of an incident
 - Establish or re-evaluate a communications response framework as part of a holistic incident response plan
- Within six months you should:
 - Develop scenario overviews and communications strategies for most likely security incidents
 - Test communication response function with crisis drills





Questions?

RSA CONFERENCE 2012



Edelman

**WEB:**

www.edelman.com

[www.edelman.com/expertise/practices/data security & privacy](http://www.edelman.com/expertise/practices/data%20security%20&%20privacy)

**TWITTER:**

EdelmanDSP

**BLOG:**

www.EdelmanDSP.com

**CONTACTS:**

Harlan Loeb
harlan.loeb@edelman.com

Leigh Nakanishi
leigh.nakanishi@edelman.com