RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Surviving A Security Firestorm: Tales From Those Who've Lived Through It

SESSION ID: CISO-W03

Moderator: Ronald Woerner
Director, Cybersecurity Studies, Bellevue University
@ronw123

Panelists: Bill Downes
CISO & VP CTO Engineering
The Hartford Financial Services Group

Kostas Georgakopoulos
US Regional Manager Security IT
UBS

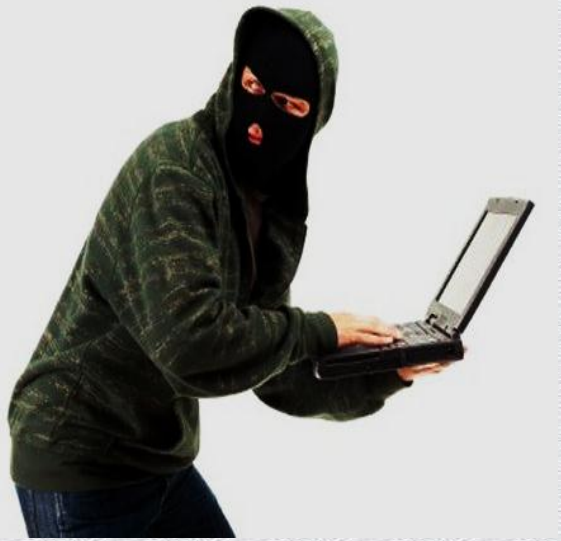
Roland Cloutier
Chief Security Officer
Automatic Data Processing, Inc.

Rocco Grillo
Managing Director Global Leader, Incident Response and Forensics Investigations
Protiviti, Inc.

Surviving A Security Firestorm – Session Overview

Hacked!

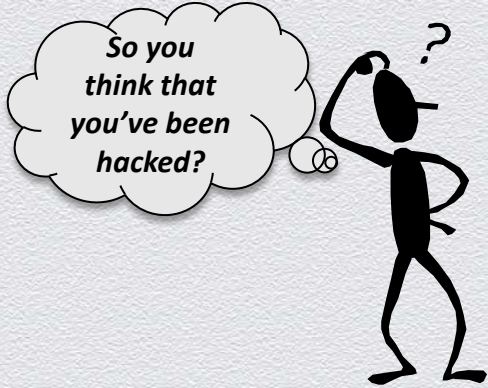
Breached! **Pwned!**



Hearing from those who have lived through it

#RSAC
RSACONFERENCE2014

Surviving A Security Firestorm



- You think you've been breached.
  - How do you know for sure?
  - Now what?
- What's your process for handing a real or potential breach?
  - Documented or undocumented?
  - Formal or informal?
  - Reaction or response?
  - How Current is Your Incident Response Plan?
    - How do you know?

What's your plan ?

#RSAC
RSACONFERENCE2014

Surviving A Security Firestorm

- To pull the plug or not pull the plug, that is the question…
- Know what you don't know before you contain
- Gathering threat intelligence to understand attack vectors
- Once We Find It, Now What?
- When is it over? When Can We Go Back to Normal?
- Lessons Learned

#RSAC
RSACONFERENCE2014

Surviving A Security Firestorm

- How do you manage the different groups involved?
  - External & Internal Communications
    - Who are the key stakeholders to involve
    - When to Discloses Publicly
    - How do you escalate?
  - Parallel activities
  - Stress

One of the leading Social Media platform announced late February 2013 that it had been breached and that data for 250,000 users was vulnerable

#RSAC
RSACONFERENCE2014

Surviving A Security Firestorm

- Who do you contact?
  - Internal
    - Legal,
    - Executive Management,
    - PR & Crisis Management
    - IT,
    - Security
    - End User Awareness
  - External
    - Outside Counsel
    - IR Handlers &Forensics Investigators
    - Private investigators,
    - Law enforcement,
    - Vendors,
    - Customers

#RSAC
RSACONFERENCE2014

Surviving A Security Firestorm

- Tools & Technologies
  - Detection
  - Response
- Logging & Auditing
  - Proactive – SOC monitoring
  - Reactive
- Forensics

#RSAC
RSACONFERENCE2014

Surviving A Security Firestorm

- Are breaches inevitable?
  - Not a matter of if, but when?
- If we can't stop them, what can we do?
- What advice do you have for a new CISO / Security Manager?

#RSAC
RSACONFERENCE2014

Surviving A Security Firestorm Session Take-Aways

- “Be Prepared”
- Know how to fail
- “Who ya gonna call?”
- Learn from it

#RSAC
RSACONFERENCE2014

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO