Security in knowledge

BATTLE SCARS AND FRIENDLY FIRE: WAR STORIES FROM A THREAT RESEARCH TEAM

Seth Geftic (@hopscast)

RSA, The Security Division of EMC

Will Gragido (@wgragido)

RSA, The Security Division of EMC

RSA CONFERENCE
EUROPE 2013

Session ID:

Session Classification:

WHAT WE HAVE LEARNED

- ▶ Building The Research Team
- ▶ Working Within Your Organization
- ▶ Our Approval Process
- ▶ Questions To Ask Before Publishing Research
- ▶ Our Research Team Survival Tips

BUILDING YOUR TEAM

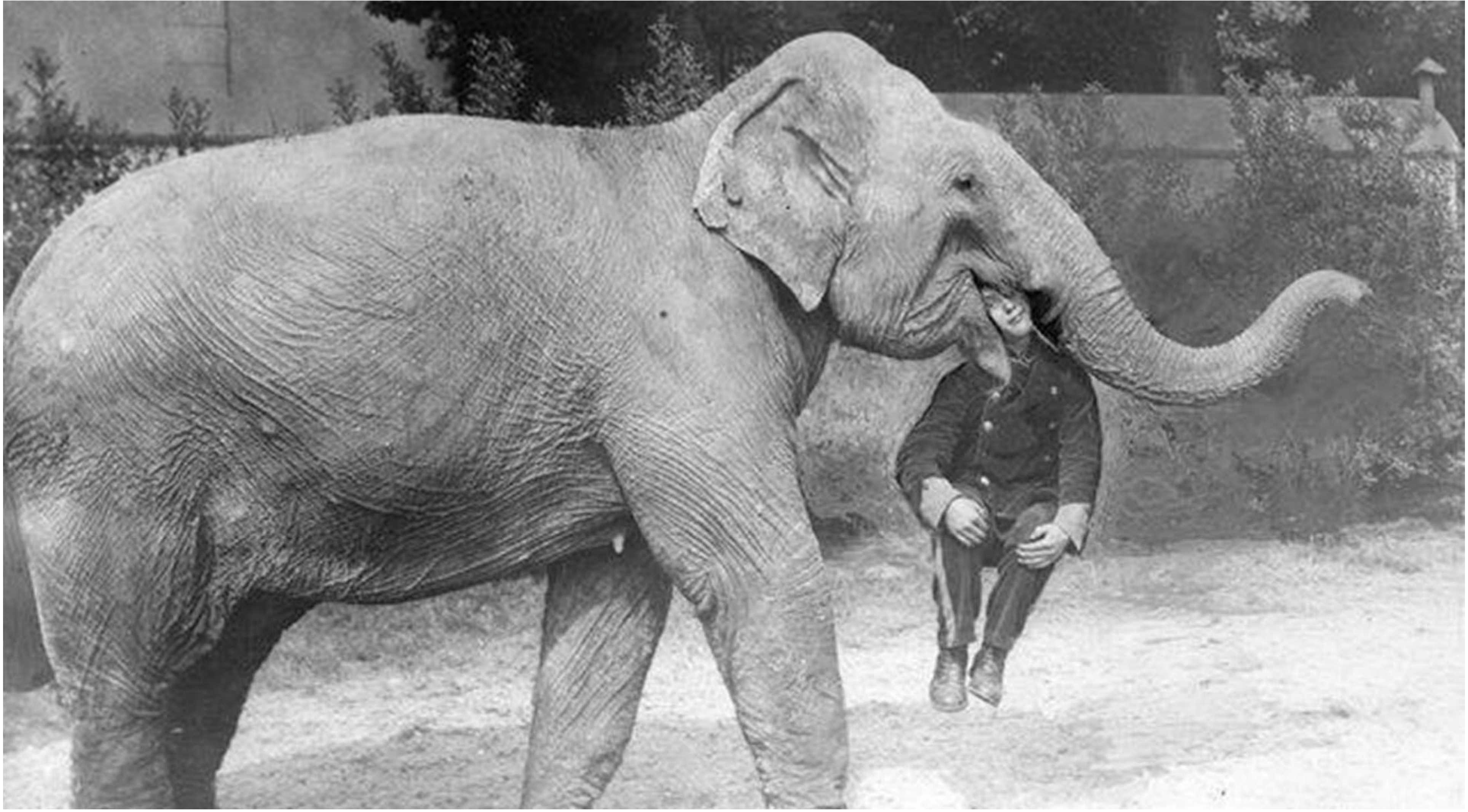
BUILDING YOUR TEAM

- Specialists vs. Generalists
  - A healthy mixture can be a good thing but requires thought
  - What are you researching?
  - Think about the big picture
  - Not all researchers are created equal
- Rogue Researcher?
  - Be on the look out for the rogue
  - Road to hell paved with good intentions

Friendly Fire

- What do various parts of your organization care about?
  - Legal
  - Market & PR
  - Sales
  - Business Executives

LEGAL



LEGAL

- Does this increase liability for the company? Are we taking on too much risk?
- Ensure no one goes to jail

MARKETING & PR

RSACONFERENCE EUROPE 2013

#RSAC

The Security Division of EMC

MARKETING & PR

- How sexy is this?
- Why are you writing about this? Why Do I care?
- Who will this resonate with?
- How will this make us look?

SALES

SALES

- How do you make me look smart?
  - Buy from us and not the competition
  - Look to us as the thought leaders
  - Make look good under all circumstances
- Don’t mess up my deals!!!!!

BUSINESS EXECUTIVES

BUSINESS EXECUTIVES

- How are you making the company money?
- Are you costing us money?
- Are you contributing to our thought leadership?
- What do you do again?

THE RESEARCHER

THE RESEARCHER

- Legitimacy
- Thought Leadership
- Integrity
- Speed & Flexibility
- Independence

Recommendations

- **Define A Research Process**
- **Understand Questions to Consider About Your Research**
- **Our Research Team Survival Tips**

OUR RESEARCH APPROVAL PROCESS

OUR RESEARCH APPROVAL PROCESS

Applies to everything external using company name (from blogs to research reports

- Draft written by researcher
  - Peer reviewed by research team and leadership
- Primary external reviewer –Product Marketing
  - Research Team needs a partner for success
- PR and Marketing team review
  - If no further reviews needed publish
- Legal team review
  - Very important if the research is made public
  - Every org will have a different risk tolerance

QUESTIONS YOU SHOULD ASK

- Where did the research data originate? Do we have written approval to use?
- Does it contain any potentially identifying information?
- Has the attack victim been notified? If not why?
- Have you notified Law Enforcement?
- Does the research contain attribution information about a specific group or nation state?
- Does the research comment on another company’s security policy?

OUR SURVIVAL TIPS

OUR SURVIVAL TIPS

- KEY TAKEAWAY: Have a written process for research approval
- Understand the motivation of your peers
  - Make their jobs easier not harder
  - Engage others as early as possible
- Seek out Executive sponsors
- Be ready to justify your existence
- Self-promote

Security in knowledge

Thank you!

Will Gragido

RSA FirstWatch Research Team

@wgragido

William.gragido@rsa.com

Seth Geftic

RSA, The Security Division of EMC

@hopscast

Seth.geftic@rsa.com
Blogs.rsa.com

Thank You!

Will Gragido
RSA FirstWatch Research Team
@wgragido and @rsafirstwatch
William.gragido@rsa.com

Seth Geftic
RSA Security Analytics
@hopscast
Seth.geftic@rsa.com

Blogs.rsa.com