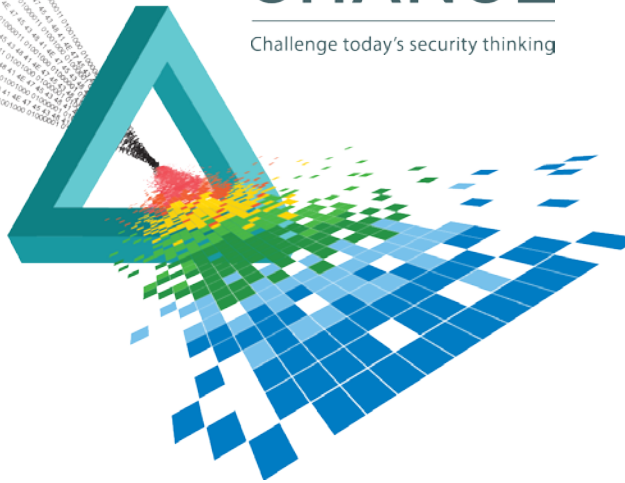
RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

CHANGE
Challenge today's security thinking



SESSION ID: SOP-R05

How to Prepare for the Worst: Don't Let Your First Crisis Be a Real One

Emilian Papadopoulos
President
Good Harbor Security Risk Management
@epapadopoulos

Tracey Pretorius
Director, Issues Management
Communications Group
Microsoft Corporation

Cyber incident response today is ad hoc, disjointed, and inefficient

- Most companies lack a plan or do not exercise it
- Response requires many organizations that have little experience working together
- Companies lack pre-arranged agreements with providers (i.e. forensics, legal, public relations, DDOS mitigation)
- The CISO ends up coordinating all the moving parts while trying to secure the network

The time to prepare is now

- Once the crisis starts, it is too late to prepare for the crisis
- You only get one try
- “It’s the planning, not the plan”

1. Understand your risks and worst case scenarios

- Work with business units to identify “crown jewels” and “worst case scenarios”
- Consider all threat actors, but focus on consequences

2. Imagine the day after

- What will your company want to have?
- What will your company want to be able to do?
- What will your company want to say, especially about its cyber security before the incident?

3. Make preparedness whole-of-enterprise

- Chief Executive Officer
- C-Suite and beyond: Finance, Operations, Marketing, General Counsel, CIO, CISO, Risk, Human Resources, Legal, Procurement, Business Units
- Employees
- Board

4. Have an incident response plan

- Define incident severity, reporting, and escalation
- Identify the crisis manager, the spokesperson, and decision/approval authorities
- Provide key steps, contacts, and decisions
- Plan against your worst-case scenarios

5. Get your team ready in advance

- Team:
  - Forensics and incident response
  - Legal
  - Public Relations
  - Breach Coach
  - Insurance

- Include your external support in planning and exercises

6. Don’t let your first crisis be a real one: practice, practice, practice

- Have the right executives at the table
- Combine multiple, cascading incidents into a tailored scenario
- Turn up the pressure: Kobayashi Maru
- Keep the scenario a surprise
- Debrief, and apply lessons learned

7. Think outside the company

- Industry approach
  - What if our whole industry was targeted?
  - What if our industry's critical supply chain was disrupted?
  - How can industry partners help?
- Consider the context

8. During the crisis

- Do:
  - Recognize a crisis
  - Remember that first reports are often wrong
  - Consider the incident ongoing until proven otherwise
  - Think about all stakeholders, including employees
  - Watch out for cockroaches
  - Have a single spokesperson
  - Prevent burnout

8. During the crisis

- Don’t:
  - Say things unless you are positive they are true
  - Wait to be called on
  - Cover up
  - Under-react

9. After the crisis

- “Fool me once, shame on you. Fool me twice, …”
- Don’t (just) fix yesterday’s problems
- Never let a good crisis go to waste

Apply: What to Do…

- Right now
  - Commit to spend 15 minutes imagining “the day after” and what you will wish you had done before a crisis hits
- Next week
  - Agree to survey business leaders and some employees for worst case scenarios, including with a “black hat” exercise
  - Ask what logs are kept, for how long, and how they are protected

Apply: What to Do…

- In the next six months
  - Write a (short) incident response plan, incorporating the worst case scenarios
  - Schedule a Table Top Exercise
  - Identify gaps in your team, and fill them
  - Launch a review of regulatory, legislative, and contractual notification requirements