TIE 2016
Resiliency Communications Exercise

Tony Perry
Senior Managing Consultant - UKI
IBM Resiliency Services
Introduction - 1

• Resiliency Communications Exercise
• Role play – coffee break and lunch – final plenary session this afternoon
• Scenario based on real incidents but simplified and compressed in time
• Learn from each other as well as our experience
• Using a crisis communications service (RCaaS) to add realism
You will receive text messages prompting you to join your team and at the end of each session.

Also plain text messages from your “subordinates” updating you (in role) on the unfolding situation.

At the end of each session please tell your facilitator:

- Which decisions you were able to make?
- What information was missing?
- What you should be communicating and to whom?

We'll take a quick overview of these in the plenary session this afternoon.
Scenario Briefing 1

You've been head hunted from your current job and taken up a senior position in a prestigious UK based organisation which sells its products and services both through intermediaries and directly to the public. You are also part of the organisation's Crisis Management Team (CMT) – whatever that is!
Scenario Briefing 2

• You are in one of four teams; each team has a room assigned to it.
• There will be an envelope with your name on it giving your role and a character briefing.
• You will receive individual messages within your role briefing you about the scenario as it unfolds.
• The facilitator in your room will send a predefined message during each session which will provide you with business status information.
• Make reasonable assumptions about the organisation and follow your character briefing on how you will react.
...Watch out for your first message!

This will work best if your mobile is connected to the internet.
TIE 2016
Resiliency Communications Exercise - explanation of what we did today and the business value

Tony Perry
Senior Managing Consultant - UKI
IBM Resiliency Services
1. Which information were you missing?
2. Which decisions were you able to make?
3. Who should you have been talking to/what should you have been telling them?
Feedback from the Teams – Session 2

1. Which information were you missing?
2. Which decisions were you able to make?
3. Who should you have been talking to/what should you have been telling them?
4. What should you say to the media?
1. Should you pay up or tough it out?
2. Should you do nothing until you've spoken to your lawyers/the police?
3. Should you say anything to the media? If so what?
Effective communications are essential in any crisis

- The cyber attack scenario was based on a number of real such events
- Rapid crisis communications and decision making are essential; this is not just an IT event.
- Having isolated IT services to support rapid communications is essential.
Resiliency Communications in context

Crisis Management = Information ▶ Decision ▶ Action

You have many stakeholders – how do you keep them informed?

Business case =

Reduced impact during a crisis + other uses

Such a tool will require changes to your incident and crisis management processes.
THE REQUIREMENT FOR A RESILIENT ENTERPRISE

INTEGRATED CYBER SECURITY FOR A NEW ERA – DELIVERING CYBER RESILIENCE

Alan Jenkins
Associate Partner, FSS/Banking & Financial Markets
Security BU, IBM UK&Ireland
AJenkins3@uk.ibm.com  +44(0)7725096098

21st September 2016
Traditional security practices are unsustainable

85 security tools from 45 vendors

1.5 MILLION unfilled security positions by 2020

68 PERCENT of CEOs are reluctant to share incident information externally
Today’s attacks require a strategic security approach

Yesterday’s Attacks
Indiscriminate malware, spam and DDoS activity

Tactical Approach
Compliance-driven, reactionary
- Build multiple perimeters
- Protect all systems
- Use signature-based methods
- Periodically scan for known threats
- Shut down systems

Strategic Approach
Intelligent, orchestrated, automated
- Prioritize high-risk assets
- Use behavioral-based methods
- Continuously monitor activity
- Gather, preserve, retrace evidence

Today’s Attacks
Advanced, persistent, organized, politically or financially motivated

It takes power and precision to stop adversaries and unknown threats
Connectivity to more users, devices, and data than ever before

It’s time to expand from infrastructure to information-centric security
How do I get started when all I see is chaos?

- Threat sharing
- Virtual patching
- Incident response
- Indicators of compromise

- IP reputation
- Network visibility
- Data access control
- Application security management
- Data monitoring

- Incident and threat management
- Content security
- Access management
- Application security management
- Entitlements and roles

- Malware protection
- Log, flow, data analysis
- Criminal detection
- Firewalls
- Antivirus

- Sandboxing
- Fraud protection
- Privileged identity management
- Application scanning
- Endpoint patching and management

- Network visibility
- Identity management
- Vulnerability management
- Transaction protection
- Cloud access security broker

- Malware protection
- Device management
- Identity management
- Anomaly detection
- Criminal detection
An integrated and intelligent security immune system
IBM Security Strategy

**SUPPORT**
the CISO agenda

- Advanced Threats
- Cloud
- Mobile and Internet of Things
- Compliance Mandates
- Skills Shortage

**ACCELERATE**
with key innovation

- Cognitive
- Cloud
- Collaboration

**LEAD**
in strategic domains

**Security Transformation Services**
Management Consulting | Systems Integration | Managed Security

**Security Operations and Response**
- Incident Response
- Security Intelligence and Analytics
- Vulnerability and Patch Management
- Endpoint and Network Protection
- User Behavior Analytics

**Information Risk and Protection**
- Cloud Security
- Mobile Security
- Identity Governance and Access Management
- Data Protection
- Application Security
- Advanced Fraud Prevention

**Security Research and Threat Intelligence**
The next era of security

PERIMETER CONTROLS

INTELLIGENCE and INTEGRATION

COGNITIVE, CLOUD, and COLLABORATION
A Global Leader in Enterprise Security

IBM Security

• #1 in enterprise security software and services*

• 7,500+ people

• 12,000+ customers

• 133 countries

• 3,500+ security patents

• 19 acquisitions since 2002

*According to Technology Business Research, Inc. (TBR) 2016
THANK YOU

FOLLOW US ON:
- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions