FIDELIS CYBERSECURITY™

PREPARE YOUR INCIDENT RESPONSE TEAM

JUNE 2015

Michael Harrington, Fidelis Cybersecurity

It's a big problem...

"The ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history."

General Keith Alexander, US Army (ret), Director of the National Security Agency, Chief of the Central Security Service, Commander of the United States Cyber Command

With no easy answers...

Overview

Critical Questions

Incident Response Expectations

Before an Incident Happens

Identify the teams of fully authorized key players

What Really Happens

How Did You Respond

Recovery

Conclusion & Questions

Critical Questions

You have been BREACHED now what?

Critical Questions

You have been BREACHED now what?

Who should be involved, who should not?

Critical Questions

You have been BREACHED now what?

Who should be involved, who should not?

Have you TRAINED for this?

Critical Questions

You have been BREACHED now what?

Who should be involved, who should not?

Have you TRAINED for this?

What are the FIRST steps and actions?

Critical Questions

You have been BREACHED now what?

Who should be involved, who should not?

Have you TRAINED for this?

What are the FIRST steps and actions?

Do you know your ROLE?

Critical Questions

You have been BREACHED now what?

Who should be involved, who should not?

Have you TRAINED for this?

What are the FIRST steps and actions?

Do you know your ROLE?

How do you handle EVIDENCE?

I.R. Expectations

Notification and Identification

I.R. Expectations

Notification and Identification

Classification: Is this a MAJOR or MINOR incident?

I.R. Expectations

Notification and Identification.

Classification: Is this a MAJOR or MINOR incident?

Know the I.R. TEAM: The People needed to respond.

I.R. Expectations

Notification and Identification.

Classification: Is this a MAJOR or MINOR incident?

Know the I.R. TEAM: The People needed to respond.

Know the Processes and Procedures & Legal and Regulatory Requirements.

I.R. Expectations

Notification and Identification.

Classification: Is this a MAJOR or MINOR incident?

Know the I.R. TEAM: The People needed to respond.

Know the Processes and Procedures & Legal and Regulatory Requirements.

3rd Party I.R. Teams and Partners

Before an Incident

Identify the team of fully authorized key players

Before an Incident

Identify the team of fully authorized key players

Know Everyone's Roles and Responsibilities

Before an Incident

Identify the team of fully authorized key players

Know Everyone's Roles and Responsibilities

Have Executive and Legal Support for the I.R. Plan

Identify the Teams of Fully Authorized Players

Leadership Team

Identify the Teams of Fully Authorized Players

Leadership Team

Legal Team

Identify the Teams of Fully Authorized Players

Leadership Team

Legal Team

Security Operations Team

Identify the Teams of Fully Authorized Players

Leadership Team

Legal Team

Security Operations Team

Forensics Team

Identify the Teams of Fully Authorized Players

Leadership Team

Legal Team

Security Operations Team

Forensics Team

Data Analysis Team

Before an Incident

TRAIN --- TRAIN --- TRAIN

Before an Incident

TRAIN --- TRAIN --- TRAIN

*** TRAIN as a TEAM ***

Before an Incident

TRAIN --- TRAIN --- TRAIN

*** TRAIN as a TEAM ***

TEST Processes and Procedures

Before an Incident

Test Your I.R. Plan > DRILL

Know Everyone's Roles and Responsibilities

Have Executive and Legal Support for the I.R. Plan

What Really Happens

What Really Happens

It is like a Circus!

What Really Happens

Critical DATA is LOST!

Evidence about the Intrusion could be DELETED!

What Really Happens

Attempts are made to limit DAMAGE so the business can run.

What Really Happens

Attempts are made to limit DAMAGE so the business can run.

A BALANCE must be made between I.R. and the Business!

How Did You Respond?

How Did You Respond?

TO: Heartbleed?

How Did You Respond?

TO: ShellShock?

How Did You Respond

Most organizations were scrambling around.

How Did You Respond

Most organizations were scrambling around.

If your security staff responded quickly and efficiently
then I commend you.

How Did You Respond

Most organizations were scrambling around.

If your security staff responded quickly and efficiently
then I commend you.

What I saw in a number of companies was chaos!

How Did You Respond

Most organizations were scrambling around.

If your security staff responded quickly and efficiently then I commend you.

What I saw in a number of companies was chaos!

If you TRAINED as a TEAM and everyone knew what to do, then your 1000% better prepared than most organizations.

Keys for Breach Preparedness

Plan

Train

Drill

Repeat

Recovery

Fixed it or did we really?

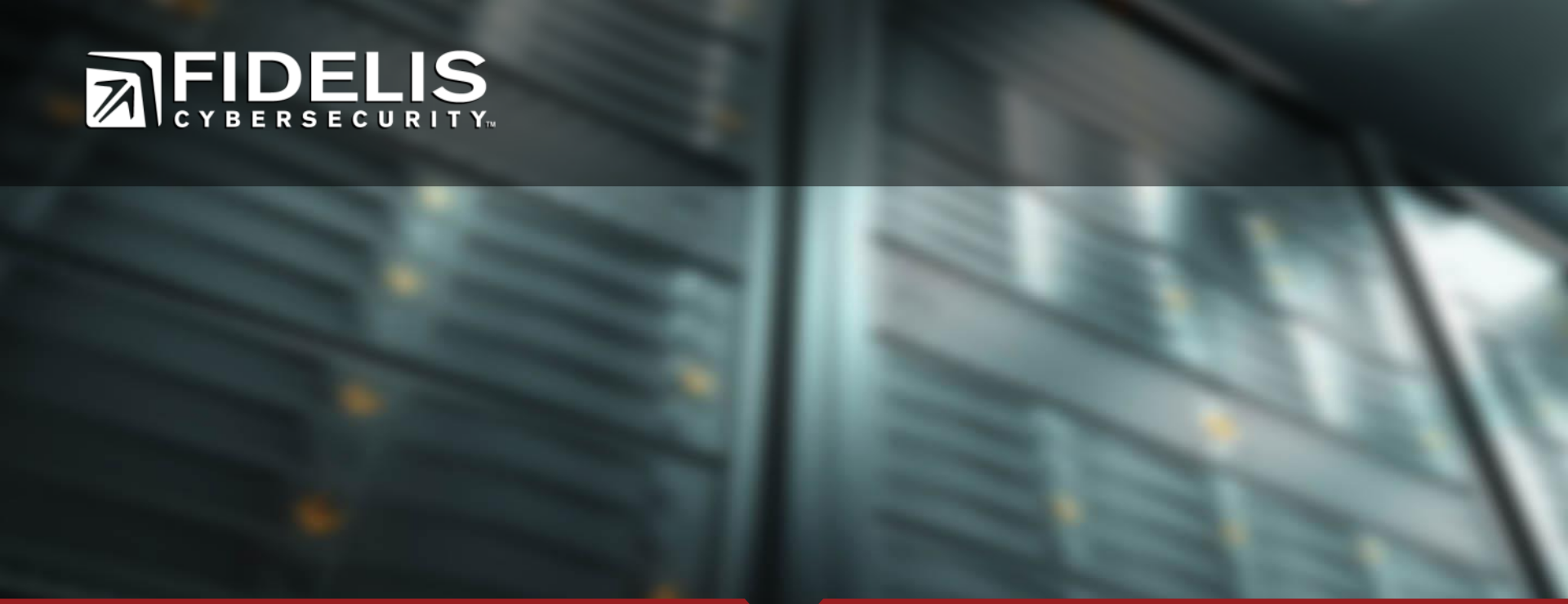
We have seen 2nd and 3rd breaches on the same customer

These were probably the same attackers hiding in wait and then they

came back out.

We Know How To Eliminate Online Risk


UP
TAIR LOCK
DOWN
CEILING
INTERNET
OFF
INTERNET
SWITCH
MUST BE ON
AT ALL TIMES
11-0866-501



QUESTIONS?

THANK YOU

Michael Harrington

Michael.harrington@fidelissecurity.com