Dissecting Data Breaches

What Keeps Going Wrong?

Powerful Insights.
Proven Delivery.®

protiviti®
Risk & Business Consulting.
Internal Audit.

02’

WHO WE ARE

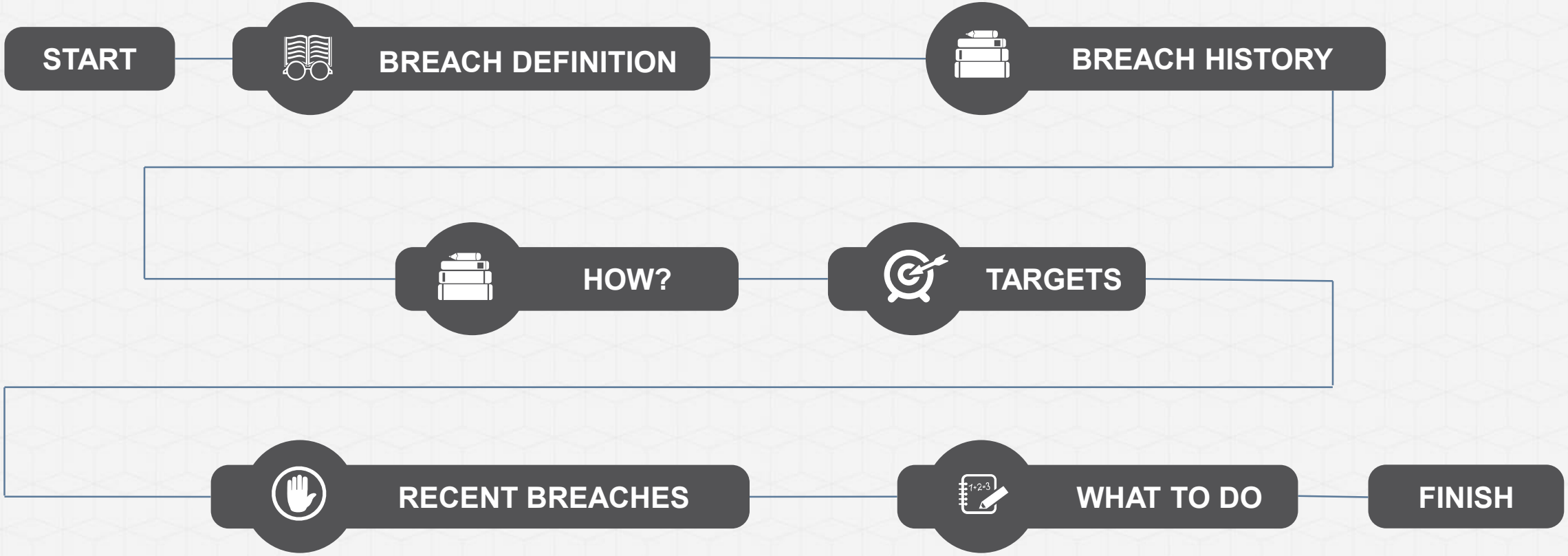
Tom Stewart

Senior Manager
IT Consulting
Protiviti

Uriah Robins

Senior Consultant
IT Consulting
Protiviti

PRESENTATION AGENDA



BREACH DEFINITON

> "A gap in a wall, barrier, or defense, especially one made by an attacking army."

A Data Breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.

BREACH HISTORY

2006

321 Reported Breaches

TJ Maxx 90 millions records exposed – Insecure wireless

2007

446 Reported Breaches

ATT 113,000 customer accts exposed Stolen laptop

2008

656 Reported Breaches

Heartland Payment systems exposed 130+ million records Malware

2009

498 Reported Breaches

US Military 76 million records Unencrypted drive returned for repair

2010

662 Reported Breaches

Sony Playstation Network 77 million Records exposed Insecure network configuration

2011

419 Reported Breaches

Apple 12 million Records exposed Poor Vendor Management

There is not just one reason for security breaches, data is leaked or lost in a multitude of ways, these are some of the biggest breaches of the last 10 years.

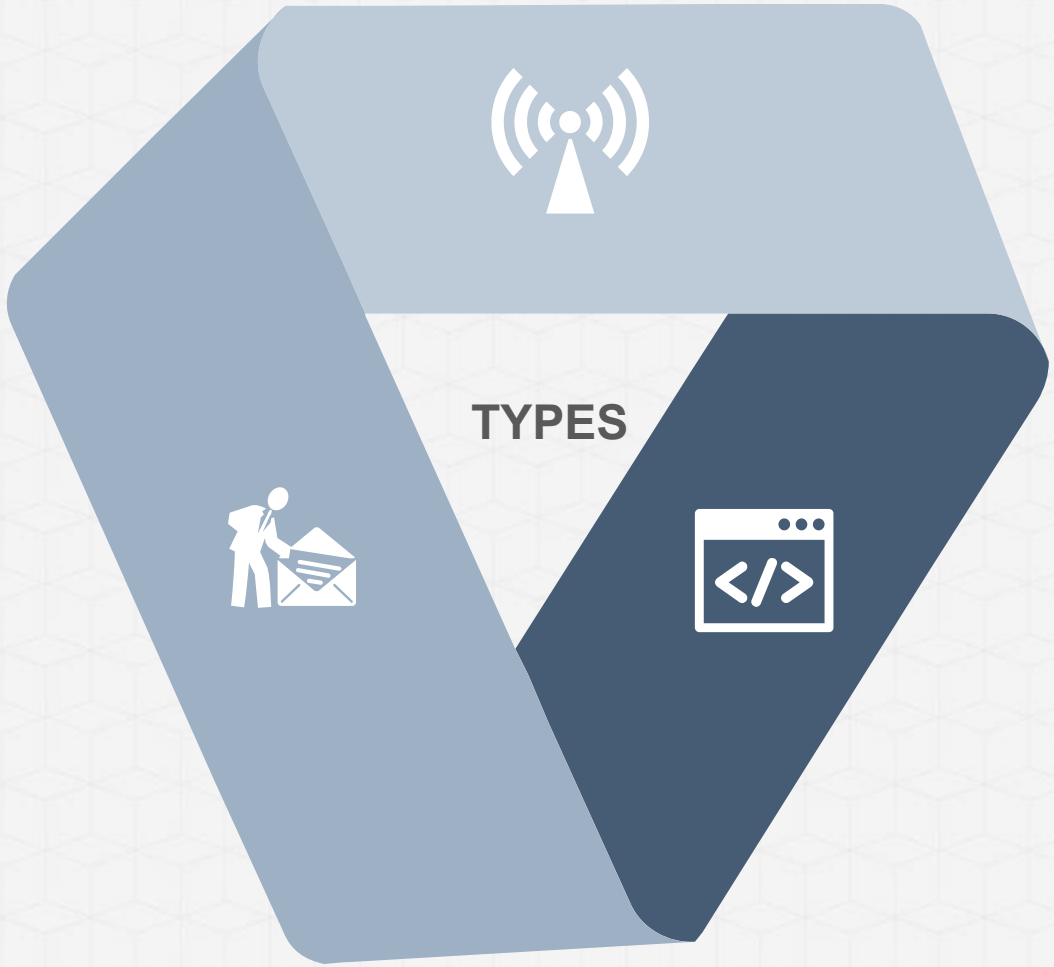
BRIEF HISTORY (Cont.)

But first, let's talk about how this happens

2012 2013 2014 2015+

THE WAY IN: HACKING

Your network is only as strong as the weakest link



VULNERABILITY EXPLOITATION

Exploiting system flaws to obtain access to data or networks

SOCIAL ENGINEERING

Exploiting human emotion to gain access to personal information

WIRELESS

Exploiting wireless flaws to remotely obtain access to data or networks

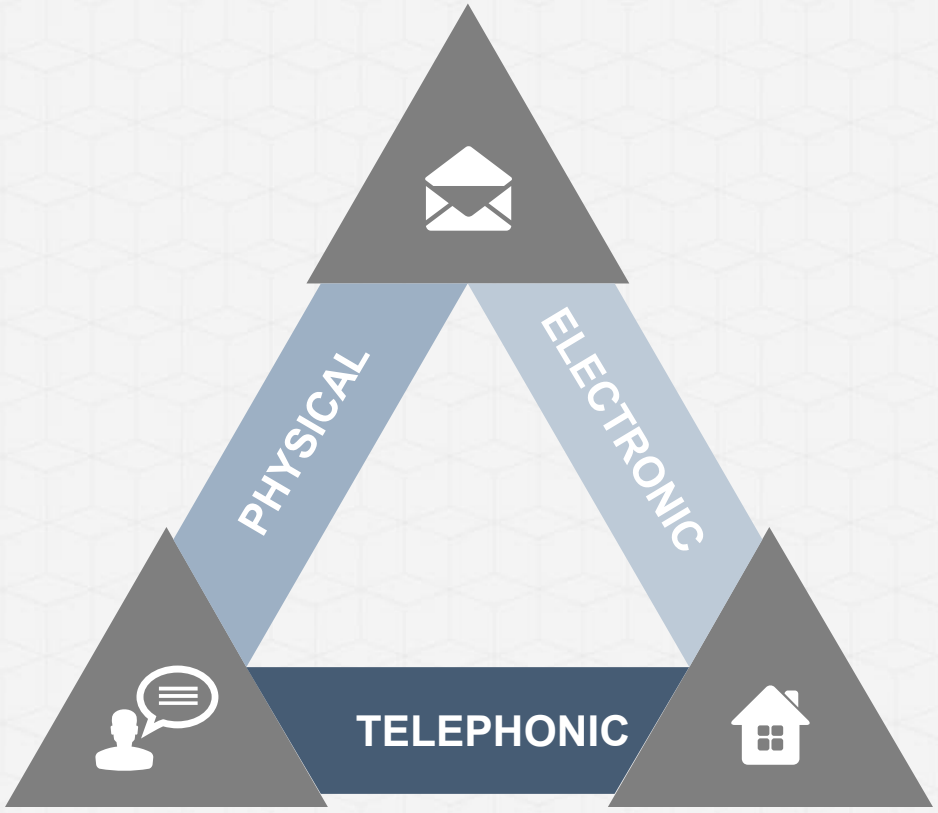
HOW THEY FIND THE HOLE: VULNERABILITY EXPLOITATION

3 STEPS TO VULNERABILITY EXPLOITATION

While exact techniques differ, modern vulnerability exploitation generally follows three set phases.

YOU ARE THE WEAKEST LINK: SOCIAL ENGINEERING

3 Types



PHYSICAL
Key Loggers
Virus Installs
Remote System Setup.

ELECTRONIC
Phishing Emails
Information Gathering

TELEPHONIC
Telephone Calls
Information Gathering

BREAK FROM A FAR: WIRELESS

01’ Major Threats

Unauthorized “Rogue” Access Points
New devices with wireless included

02’ Compromise Internal Networks

Confidentiality
Integrity
Availability

03’ Use or Disrupt Resources

Wireless DoS
Inject traffic into internal networks
Drive-by spammers

WHAT ARE THEY AFTER?

Personally Identifiable Information

- PII
- Credit Card Data
- Medical Information
- Intellectual Property
- Client Databases
- Vendor Databases

Personally Identifying Information?

- Social Security Numbers
- Birthdate
- Address

Example

Personal information stored in company databases used for credit checks.

This information can be used to open new accounts in the victims name, the better the credit score of the victim, the more valuable the data.

WHAT ARE THEY AFTER?

Credit Card Data

- PII
- Credit Card Data
- Medical Information
- Intellectual Property
- Client Databases
- Vendor Databases

Credit Card Data

- Unmasked Credit Card Numbers
- Stripe Data
- CVV Codes

Example

Unmasked credit card data stored in databases for use at a future date.

Credit card numbers and strip data can be sold on the black market. Prices vary based on credit score of the individual, available credit and type of card and strip data captured.

WHAT ARE THEY AFTER?

Medical Information

- PII
- Credit Card Data
- Medical Information
- Intellectual Property
- Client Databases
- Vendor Databases

Medical Information

- Blood Type
- Medication Lists
- Treatment History
- Family History

Example

Medical history can be used for blackmail purposes, targeted attacks or simply building a dossier on an individual for later use.

WHAT ARE THEY AFTER?

Intellectual Property

- PII
- Credit Card Data
- Medical Information
- Intellectual Property
- Client Databases
- Vendor Databases

Intellectual Property

- Algorithm
- Source Code
- Research

Example

An encryption algorithm, source code for the latest game engine or research being conducted at a pharmaceutical firm, are all likely targets of a data breach.

WHAT ARE THEY AFTER?

Client Databases

- PII
- Credit Card Data
- Medical Information
- Intellectual Property
- Client Databases
- Vendor Databases

Client Databases

- Client personal information
- Physical addresses
- Email addresses

Example

Client databases are stolen and sold for personal information dumps (for use in identity theft or other purposes) as well as targeted client lists to be sold to competitors.

WHAT ARE THEY AFTER?

Vendor Databases

- PII
- Credit Card Data
- Medical Information
- Intellectual Property
- Client Databases
- Vendor Information

Vendor Databases

- Parts lists - suppliers and costs
- Services – suppliers and costs

Example

Vendor Databases often contain parts suppliers and pricing for manufactured goods, this information is invaluable for competitors attempting to get an upper hand.

BRIEF HISTORY (Cont.)

2012

447 Breaches Reported

Living Social 50 million records exposed

Insecure Network Configuration

2013

614 Breaches Reported

Zappos 24 million records

Poor Input Sanitization

2014

753 Breaches Reported

Sony $300+ million

Lost records

Insider threat

2015+

What's Next

Back to the fun stories…

4 SIMPLE STEPS

Where to go from here.

01 **ALIGN WITH A STANDARD**
Secure systems and improve processes

02 **USER ACCESS MANAGEMENT**
File Shares, Applications, Vendors

03 **PROACTIVE TESTING**
Simulated penetration testing and vulnerability assessments for low hanging fruit

04 **INDEPENDENT 3RD PARTY REVIEWS**
Verification of ongoing processes

20’

Q & A

Tom Stewart

Senior Manager
Information Security
Protiviti

Uriah Robins

Senior Consultant
IT Consulting
Protiviti