



**Wespath**

BENEFITS | INVESTMENTS



CONFERENCE FORUM

**Working in Partnership  
to Protect Our Data  
Cyber Security**

# Agenda

- Cyber Security Landscape
- Primary Methods of Attack and Best Practices for Prevention
- What's Coming
  - Benefits Access for Plan Sponsors
  - Secure Messaging
- What Can We Do to Support You?

The source for information in this presentation is the *Verizon 2016 Data Breach Investigations Report*, unless otherwise indicated.

# Cyber Security



**We're All In This Together!**

Wespath, plan sponsors  
and participants—  
critical links in a chain  
that must not be broken

**We MUST be persistent  
in our protection efforts!**

# Cyber Attacks—Notable statistics



<b>89%</b>	Of attacks involve <b>financial</b> or espionage motivations
<b>63%</b>	Of confirmed data breaches involve using <b>weak, default or stolen passwords</b>
<b>85%</b>	Of all exploited vulnerabilities resulted from the <b>top 10 known vulnerabilities</b> —often months or years after patch was published
<b>\$40</b>	Median cost per lost record in a data breach (Total costs: \$35K - \$1.6M)*
<b>13%</b>	Of users fall for phishing—opening e-mails
<b>16%</b>	Increase in ransomware attacks over 2015

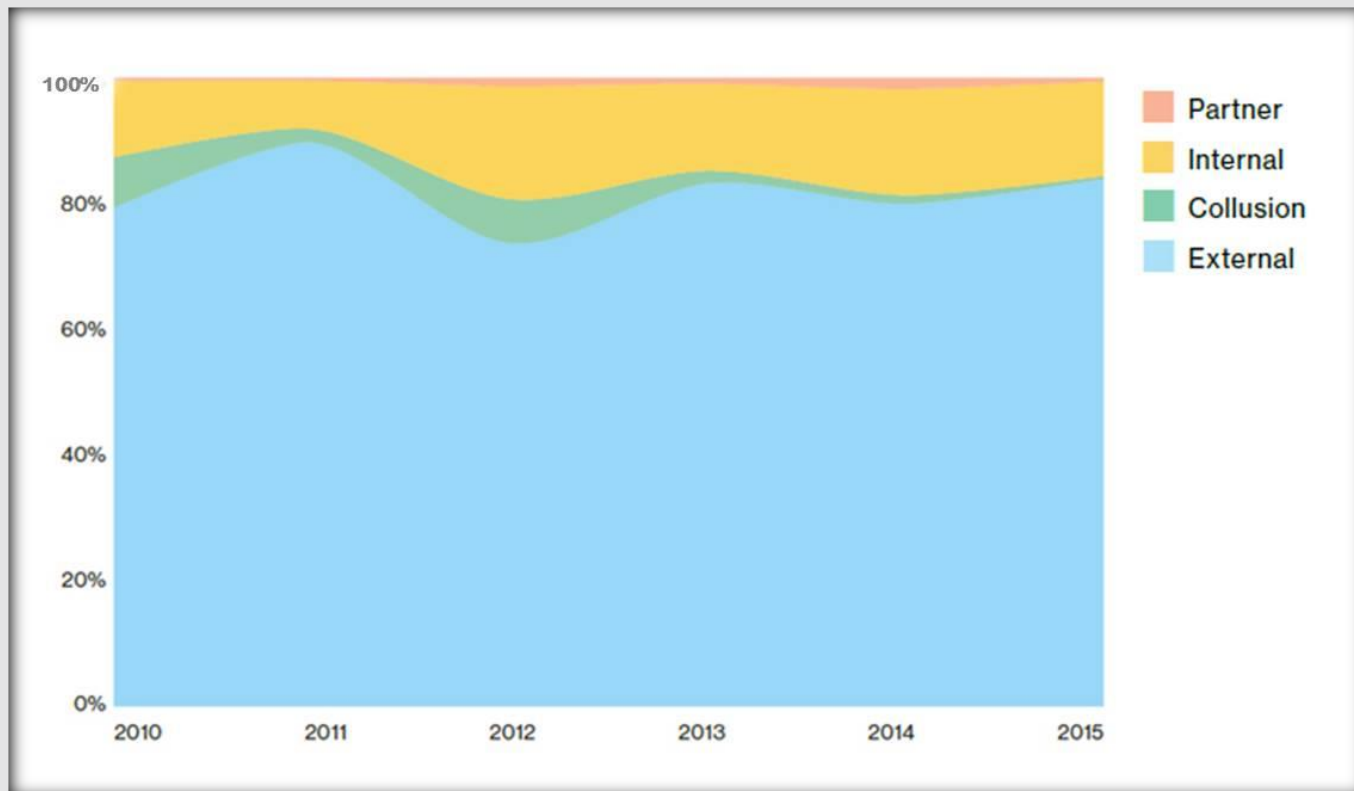
\* Source — Net Diligence 2016 Cyber Claims Study

# Global Impact



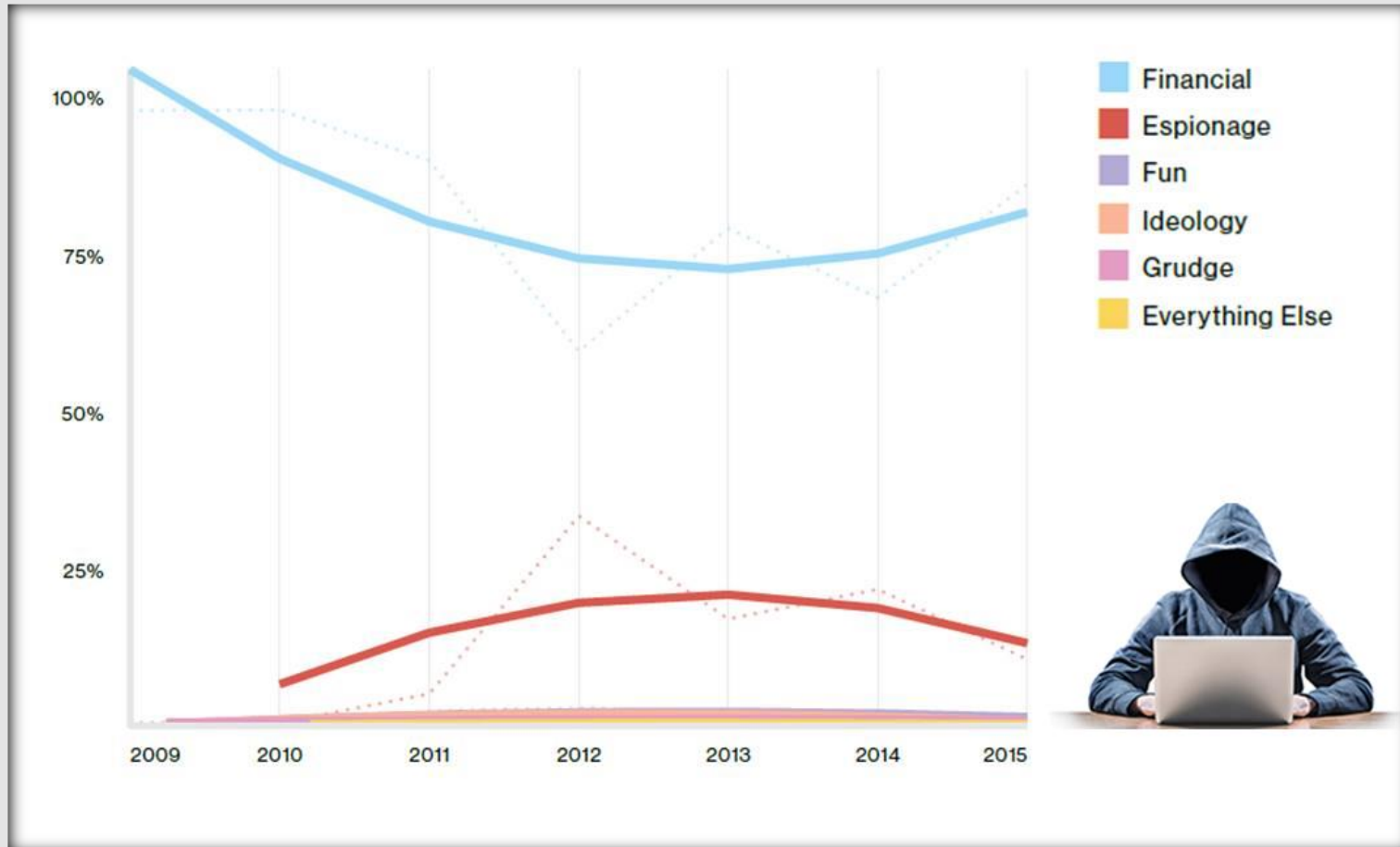
**82 countries and myriad of industries impacted**

# Actors Predominantly External

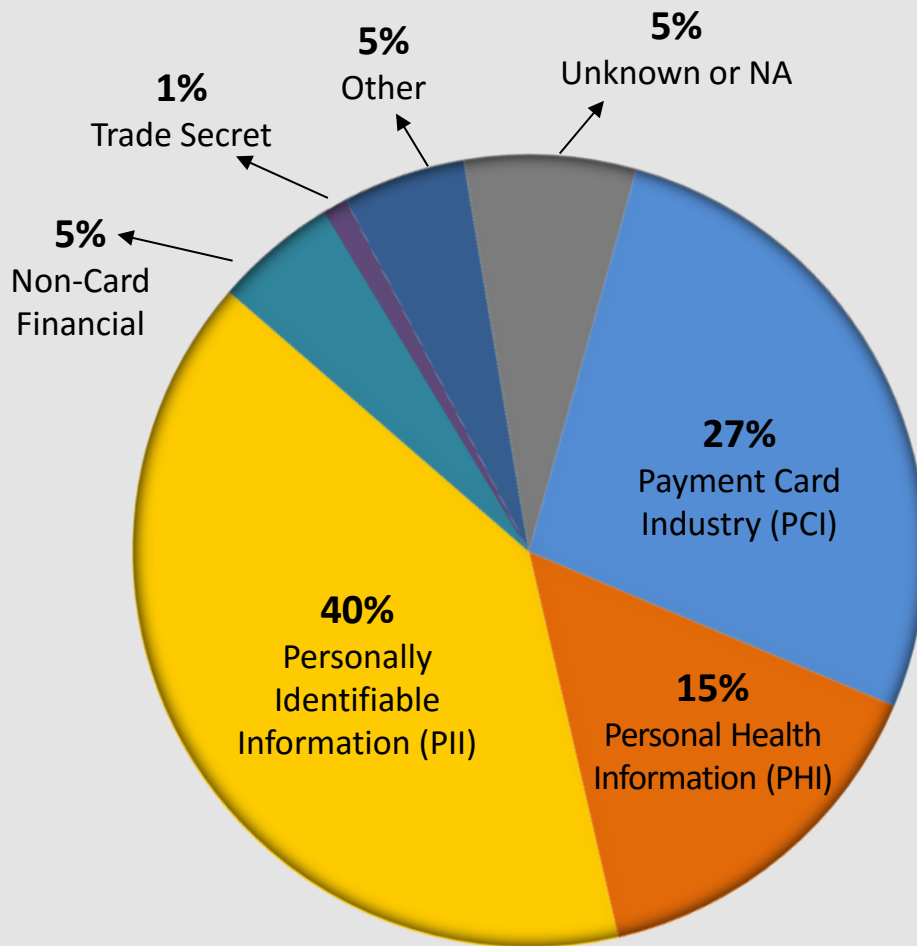


**Let's face it, there are more people outside your conference than there are inside it.**

# Why Are They Hacking?



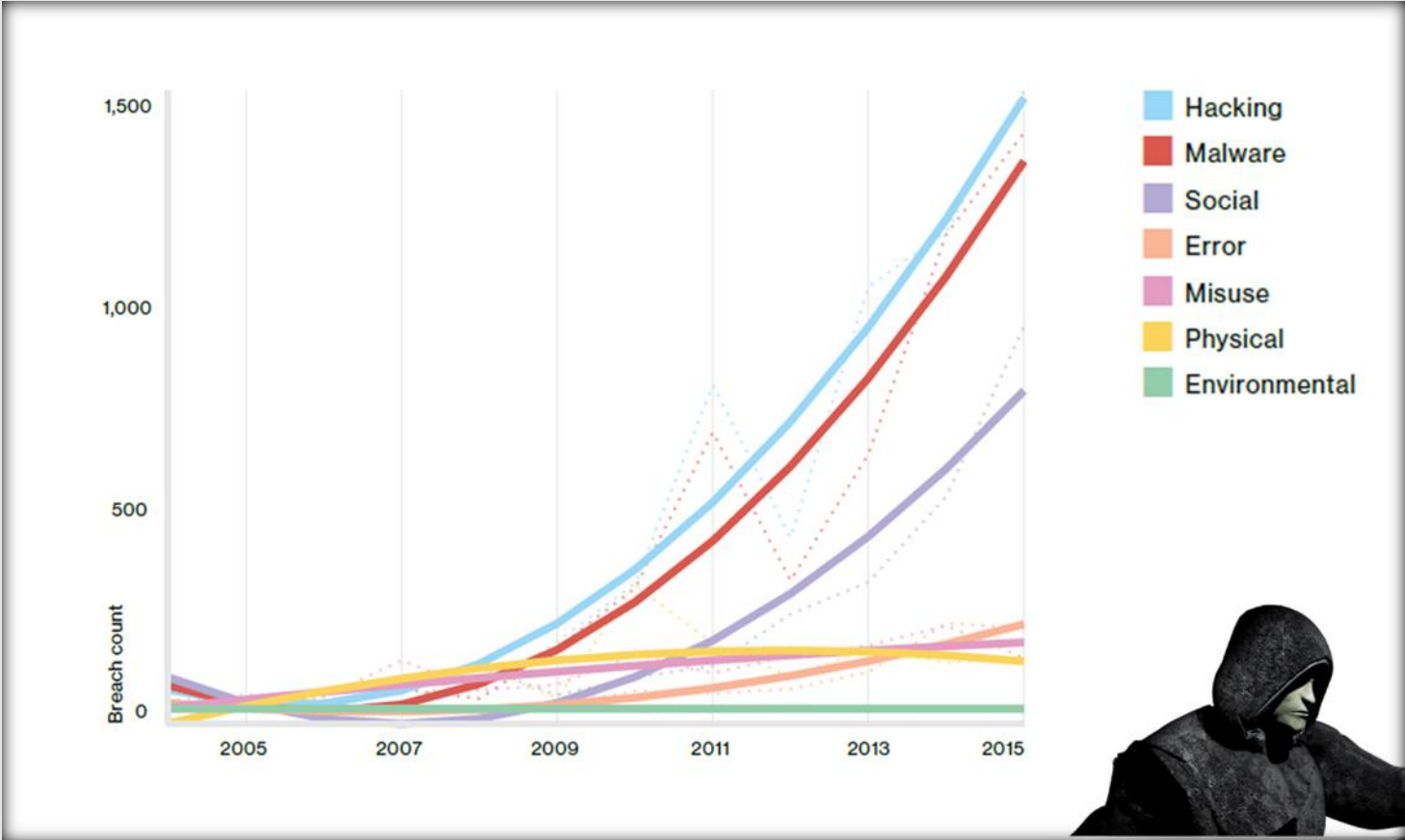
# What Are They Trying to Access?



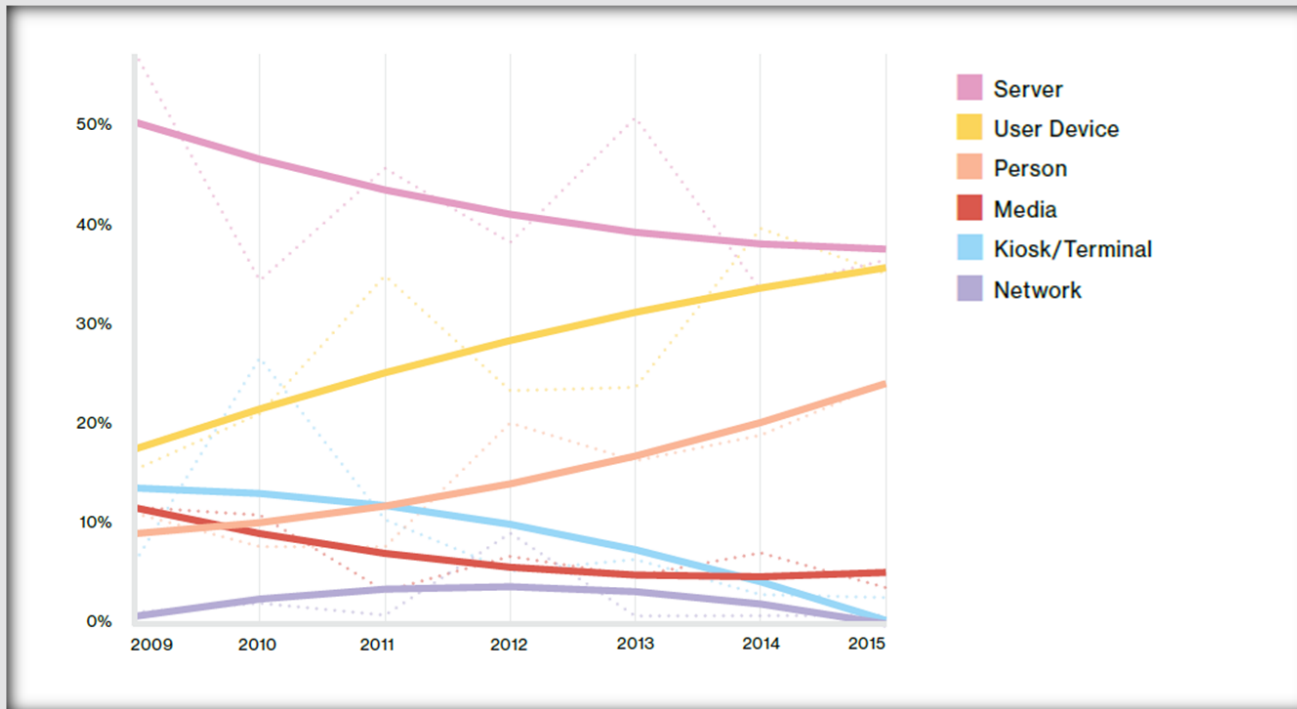
**55%** of hackers  
attempting to access  
**PHI and PII**



# How Are They Doing It?



# How Are They Doing It?



**As IT adds more defenses, hackers are becoming more focused on the human element**

# Prominent Methods of Attack: System Exploits



## What Is It?

- Via exposed vulnerabilities in your network or applications
- Criminals gain access to private computer systems
  - Gather sensitive personal information (Social Security numbers, account numbers, passwords, etc.)

## How Do They Do It?

Denial-of-service attacks, application or network attacks, gaining administrative privileges or capturing credentials.

# Multi-Pronged Approach: System Exploits



## Be Diligent in Vulnerability Management

- New vulnerabilities identified every day
- Older vulnerabilities still heavily targeted
- A methodical patch approach emphasizes **consistency and coverage**—patching the right things is more important than expedient patching
- Have a plan B for systems that can't be patched
- Run vulnerability scans or hire a service to do it for you

# Prominent Methods of Attack: Phishing



## What Is It?

- Via e-mail
- Criminals acquire sensitive personal information directly from the user or via malware

## How Do They Do It?

Masquerading as an entity with which the victim already has a relationship (e.g., bank, credit card company, brokerage company or other financial services firm), the criminals solicit ***sensitive personal data*** from unwitting recipients

# Multi-Pronged Approach: Phishing

- Be diligent filtering e-mail
- Provide employees with awareness training
- Don't fall victim to employee "clicks"
  - Layer your defense
  - Segment your network
  - Implement strong authentication
  - Monitor traffic
  - Deploy a solid security suite Anti-X (malware, spyware, ransomware and virus protection)



**Wespath will never ask for your account password via the phone or e-mail.**

# Prominent Methods of Attack: Authentication



## What is it?

Use of stolen credentials and other hacking and malware actions targeting traditional username and password authentication

## How do they do it?

Criminals acquire user ID and password via key loggers, malware, purchase in the black market, systematic attempts to crack weak or reused passwords.

# Multi-Pronged Approach: Authentication

- **Insist on STRONG Password Policies**
  - Complexity
  - Length
  - Age
  - Reuse
- **Rely on multi-factor authentication**





# Wespath's Framework of Protection

## Customer Protection



## Enterprise Risk Management



## Validating Results



# What's Coming— Benefits Access for Plan Sponsors

## Additional Protections

- Multi-factor authentication
- Threat layers
- Data masking
- Secure message center

## Improved usability

- Batch functions
- Service and compensation
- Reporting



Strengthened Security



Improved Usability

**Attend the BAP break-out session to learn and see much more!**

# Cyber Security

## The risk for a hack is real!

Wespath has received fraudulent requests—e-mails and calls from actors attempting to portray some conference personnel.

Our controls detected and prevented these attempts.

We must be in partnership—  
protecting our data!



# What Can We Do to Support You?



**Things you would like us to consider**

**Questions**



**Wes**path

BENEFITS | INVESTMENTS