Shouldn't your "Incident Response"
be "Instant Response?"
CyFIR

Madness

ASHLEY MADISON®
Life is short. Have an affair.®

SONY
make.believe

TARGET

CHS Community Health Systems

THE HOME DEPOT

ebay

Adobe

First Data
beyond the tran

Neiman Marcus

TACO BELL

Marriott

IRS

KASPERSKY lab

Kroger

BlueCross BlueShield

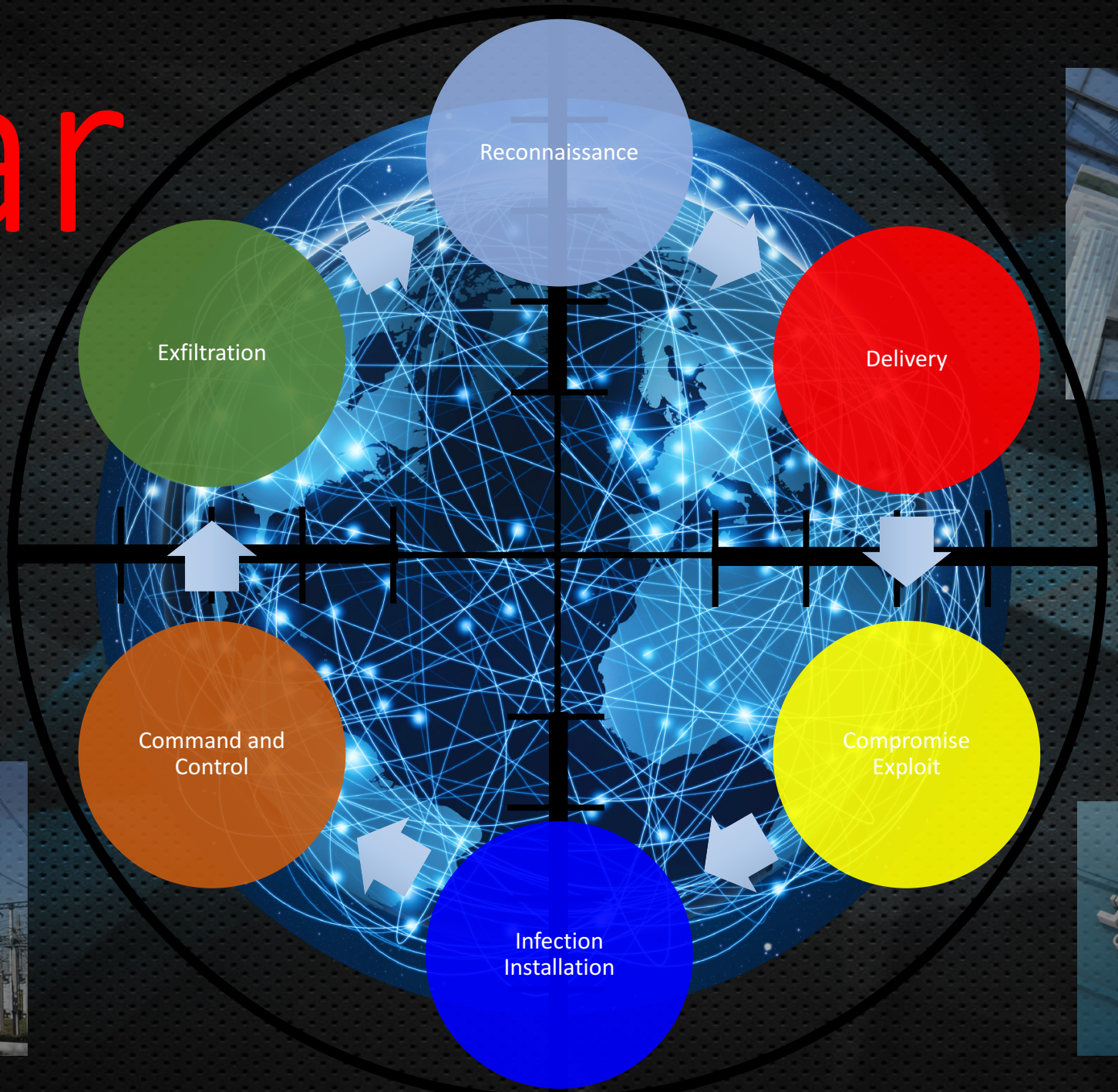
NBC

Schnucks

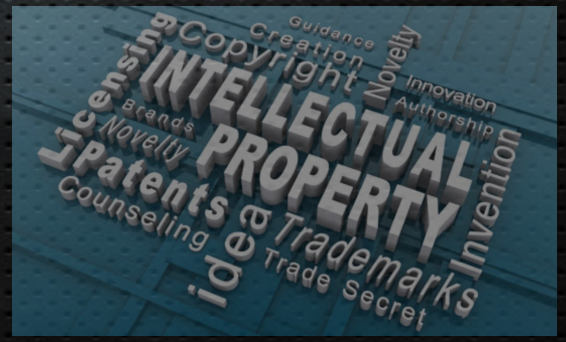
Madness

- 2007 – BlackEnergy Malware Developed
- 2014 - 17 Power Related Companies Breached (including 4 Utilities)
- Dec 2012 – 2 US Power Plants Breached
- Dec 2015 – Ukraine Power Grid Hacked/Brought Down
- 317 Million New Malware Variants in 2015

War


Reconnaissance
Delivery
Compromise
Exploit
Infection
Installation
Command and
Control
Exfiltration

BANK

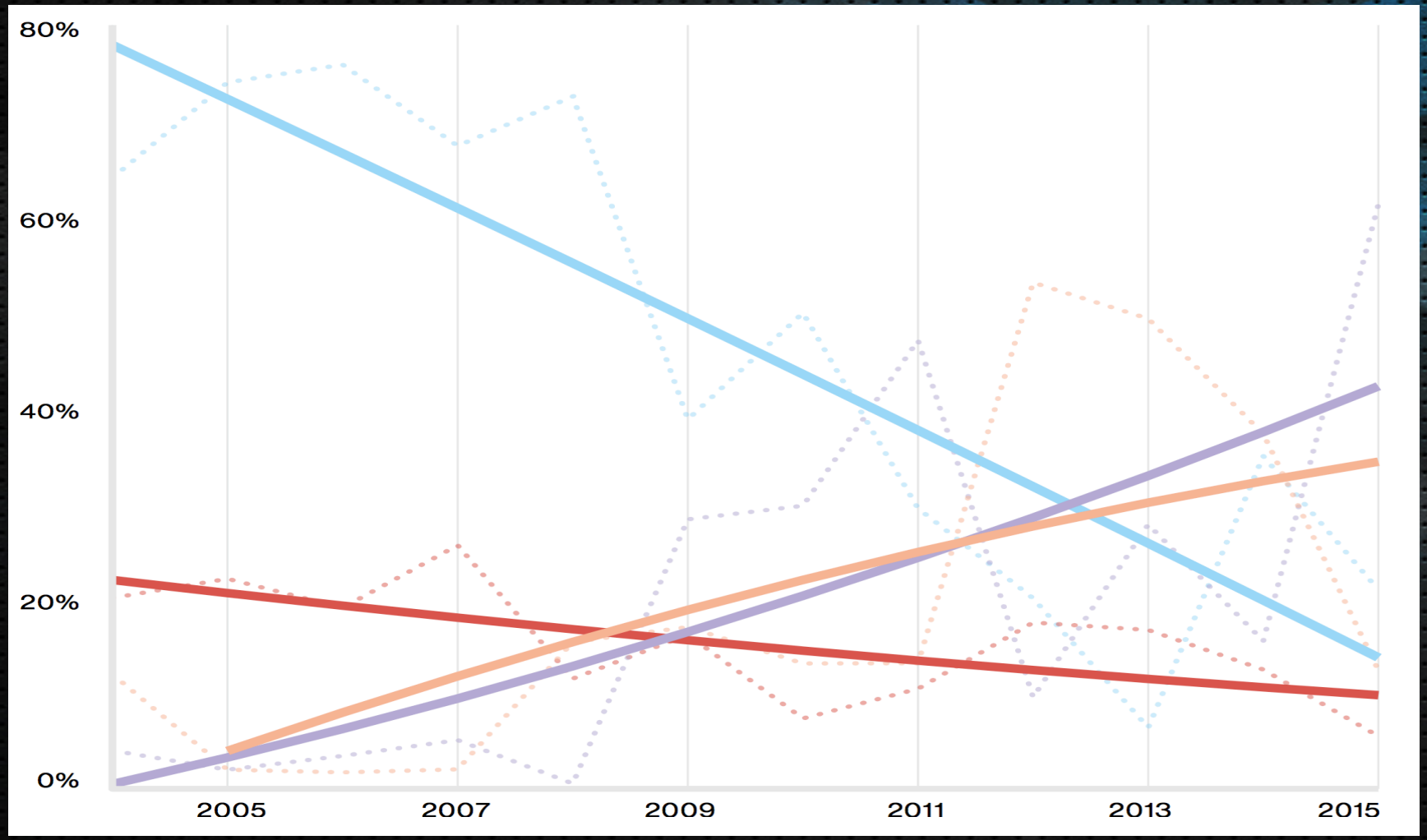

Guidance
Creation
Copyright
Novelty
Licensing
Innovation
Authorship
INTELLECTUAL
PROPERTY
Brands
Novelty
Invention
Patents
Trademarks
Counseling
Trade Secret

$75.4 Billion

$18 Billion

Reality

Breach Detection Sources



Reality

96%
Of breaches Involve Unauthorized Programs on The End Point

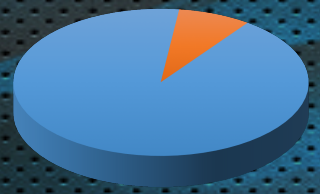
Known External Actors

55%
Organized Crime

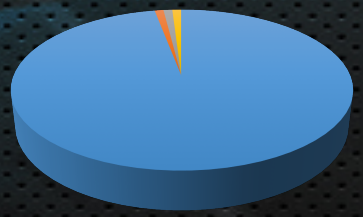
21%
State affiliated

2%
Activist

1%
Former employee



92%
Of breaches are perpetrated by outsiders



97%
Of companies *Are Breached, the Majority from Special Purpose Malware*

Who found the incident

Outside party

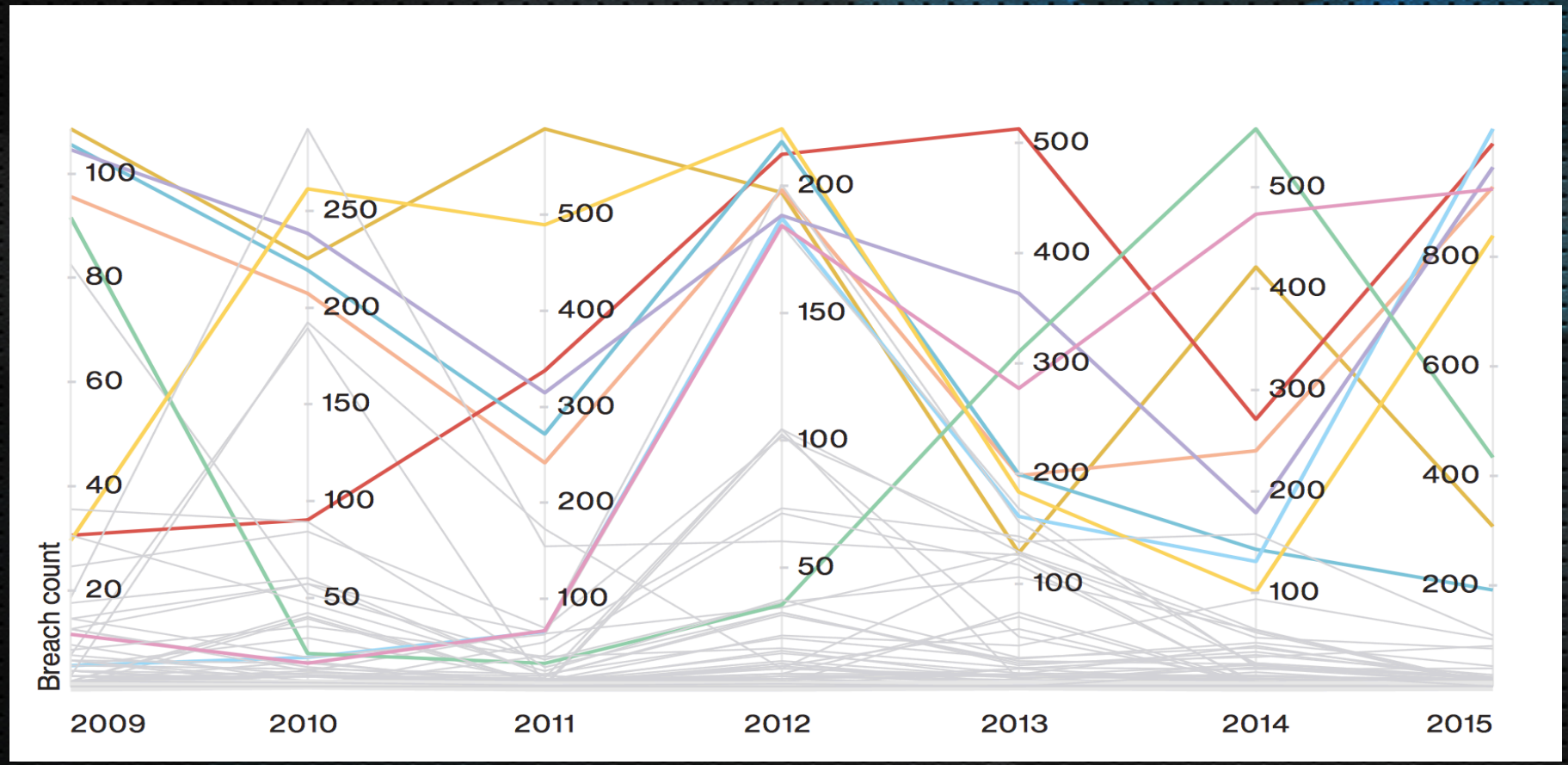
Customer

Business partners

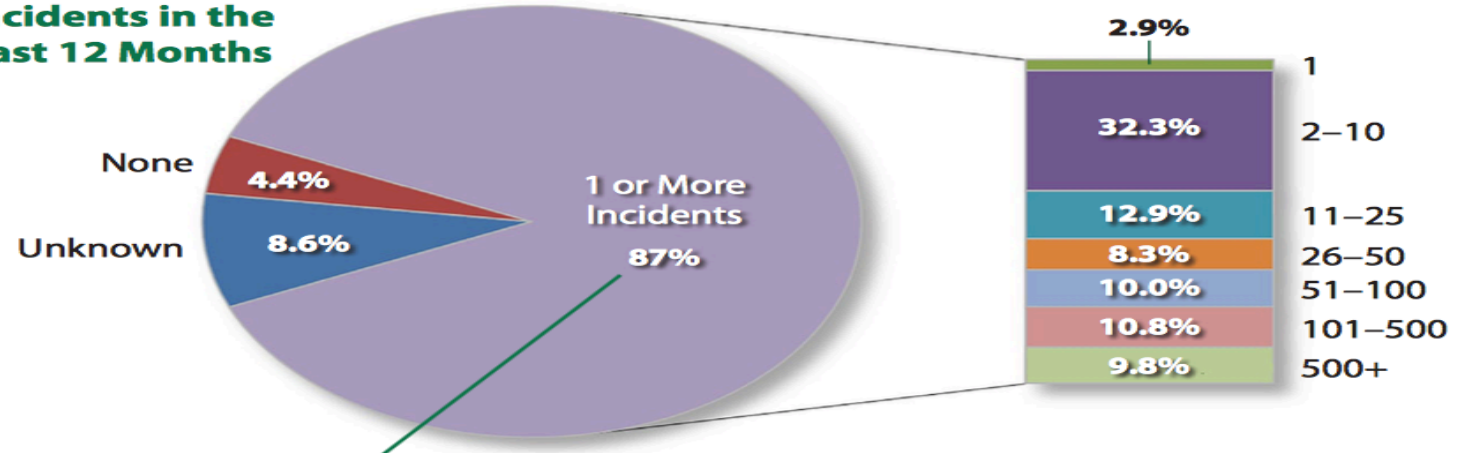
IDS

Reality

Hackers Will Find a Way.....

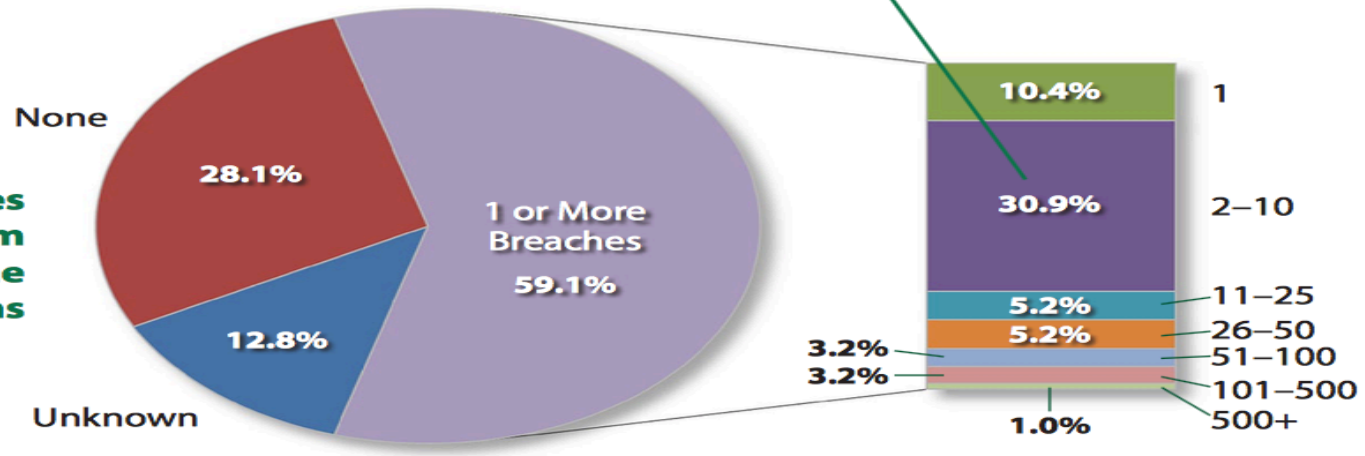


Incidents in the Past 12 Months



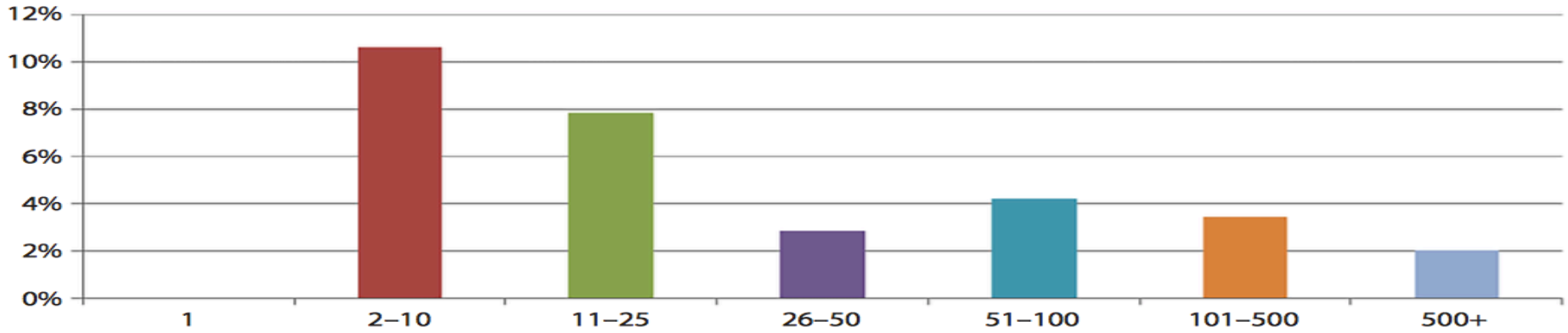
87% reported incidents in the past 12 months, and these incidents resulted in actual breaches 59% of the time.

Actual Breaches Resulting from Incidents in the Past 12 Months

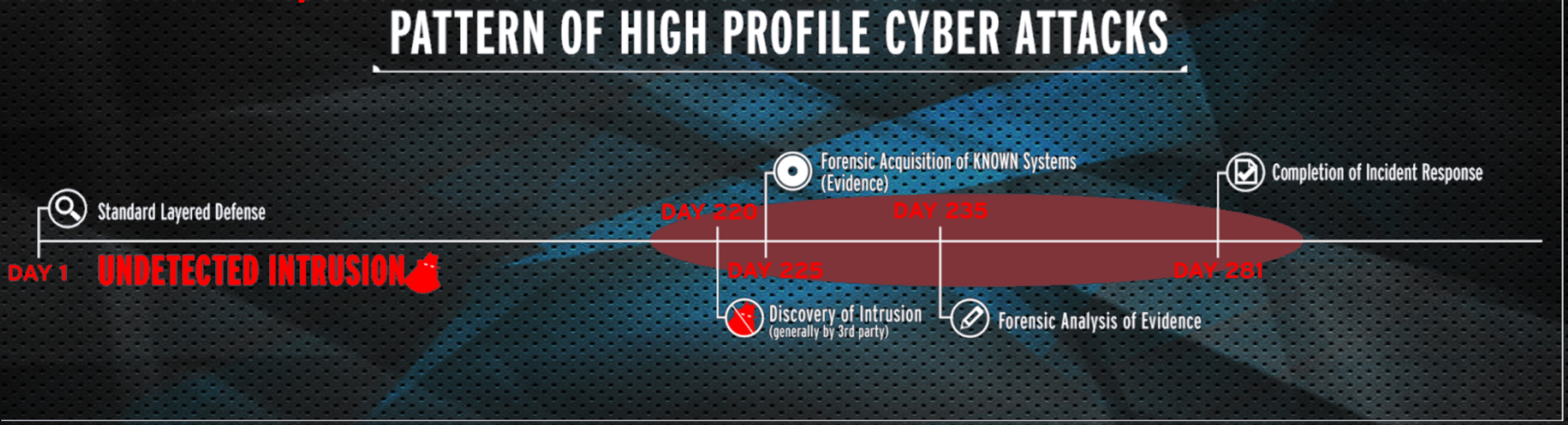


Almost 31% experienced between 2 and 10 breaches, the majority of which came from 2 to 10 incidents.

Number of Incidents that Resulted in 2 to 10 Breaches



Reality Sucks



Compliance is not Capability!!!!!

These tools are FISMA, PCI, and HIPAA Compliant

<u>But They Won't Help You with APT!</u>

Some Uncomfortable Questions……

10 Years After the Discovery of Power Grid Specific Malware:

- Do you know every process/program that is running in your network?
- Are you relying on obscurity to provide security?
- Have you identified all your vulnerability points?
- What are you doing about physical security, EMP?
- How fast can you remediate a situation?
- When have you truly tested your security TTP's?

Think Asymmetrically About the Problem

Motivators

- Money
- Prestige
- Political
- Military

Strengths

- Motivated
- Patient
- Well Funded
- Talented

Weaknesses

- Dev Time/Costs
- Communications
- Dev Costs
- Individual Specific Capabilities

Technology, Training and People are Necessary to Defeat the Adversary

….And Change the Way We do Business

Current State

- Reactive
- Lack of Endpoint Visibility
- Extremely Poor Alert Context
- Heavy Reliance on Off Line Analysis
- Heavy Reliance on Manual Process
- Fragmented Toolsets
- Obsolete Procedures
- Compliant, But not Capable

NextGEN

- Proactive Hunting
- Complete-Real Time Endpoint Visibility
  - 100% Process Identification
  - Live RAM Analysis
  - Live HD Analysis
- Instant Response
- Live Response – No need to Fly In SME
- Big Data Analytics

Speed to Resolution (S2R)

- Time from Discovery to Remediation
- Dependent on:
  - People
  - Process
  - Tools
- S2R Using Legacy Industry Tools is 10 Months
- NextGen CyFIR S2R = Minutes

IT'S
ABOUT
TIME